



BIPAC 7100SV

VoIP ADSL Modem/Router

with Single Ethernet Port

User Manual

Table of Contents

Chapter 1	1
INTRODUCTION	1
1.1 An Overview of BIPAC 7100SV	1
1.2 Package Contents	2
1.3 BIPAC 7100SV Features.....	2
1.4 BIPAC 7100SV Application	4
Chapter 2	5
USING BILLION VOIP ADSL MODEM/ROUTER	5
2.1 Cautions for Using Billion VoIP ADSL Modem/Router	5
2.2 The Front LEDs.....	5
2.3 The Rear Ports.....	6
2.4 Cabling.....	6
Chapter 3	7
CONFIGURATION	7
3.1 Before Configuration	7
3.2 Factory Default Settings	14
3.2.1 Password	15
3.2.2 LAN and WAN Port Addresses	15
3.3 Information from ISP	15
3.4 Configuring with Web Browser	16
3.4.1 Status.....	17
3.4.1.1 Status – ADSL Status	18
3.4.1.1.1 ADSL Status – WAN Status	19
3.4.1.1.2 ADSL Status – ATM Status	19
3.4.1.2 Status – LAN Status.....	20
3.4.1.2.1 LAN Status – TCP Status	21
3.4.1.3 Status- PPP Status.....	21
3.4.1.4 Status- Learned MAC Table	22
3.4.1.5 Routing Table.....	22
3.4.1.6 System Log.....	23
3.4.1.7 Security Logs.....	24
3.4.2 Quick Start	24
3.4.2.1 ADSL Quick Start	24
3.4.2.2 VoIP Quick Start	25
3.4.3 Configuration.....	26
3.4.3.1 WAN	26
3.4.3.2 LAN.....	29
3.4.3.3 VoIP	30
3.4.3.3.1 Configuration	31
3.4.3.3.2 Service Provider	32
3.4.3.3.3 Phone Book	33
3.4.3.3.4 Dial Plan	34
3.4.3.3.5 Call Feature	34
3.4.3.3.6 PTM.....	36

3.4.3.3.6 Ring Tone	36
3.4.3.3.7 Timer	38
3.4.3.4 System	39
3.4.3.4.1 Password.....	39
3.4.3.4.2 Time Zone	40
3.4.3.4.3 Upgrade.....	41
3.4.3.4.4 Factory Setting	42
3.4.3.4.5 Restart.....	42
3.4.3.5 Firewall.....	43
3.4.3.5.1 Packet Filtering.....	43
3.4.3.5.2 Bridge Filtering	45
3.4.3.5.3 Intrusion Detection.....	46
3.4.3.5.4 Block WAN Request	47
3.4.3.6 Virtual Server.....	48
3.4.3.7 Advanced.....	49
3.4.3.7.1 ADSL	49
3.4.3.7.2 DNS.....	50
3.4.3.7.3 Dynamic DNS.....	51
3.4.3.7.4 NAT	52
3.4.3.7.5 RIP	54
3.4.3.7.6 Static Route.....	55
3.4.3.7.7 MISC Configuration	56
3.4.3.7.8 Diagnostic Test.....	57
3.4.4 Save Config	60

Chapter 4..... 61

TROUBLESHOOTING 61

Problems Starting Up the ADSL Router	61
Problems with the WAN Interface	61
Problems with the LAN Interface	61
Problems Connecting to a Remote Node or ISP.....	61

APPENDIX..... 62

PRODUCT SUPPORT AND CONTACT INFORMATION..... 62

1.1 An Overview of BIPAC 7100SV

BIPAC 7100SV VoIP ADSL Modem/Router provides a high-speed Ethernet port for high-speed Internet browsing. It can support downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2); G.hs (G994.1)).

The product supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with ISP. The product also supports VC-based and LLC-based multiplexing.

It is the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user's network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides two levels of security support. First, it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly, it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, user can open some specific ports for outside users to access internal services in network.

Integrated DHCP (Dynamic Host Control Protocol) services, client and server, allow multiple users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server and reboot. Each time local machine is powered up; the router will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP (Internet Service Providers) provided IP address can be set to the product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

BIPAC 7100SV serves as a Public Switched Telephone Network (PSTN) handset-to-Ethernet adaptor that enables traditional telephone devices to operate as Internet Protocol (IP) devices. It is the interface

between the PSTN world and the IP world acting as a residential gateway, eventually providing Internet Telephony capability. Cost savings and ease of developing and integrating new services motivate most of the interest in Internet telephony. Internet telephony integrates a variety of services provided by the current Internet and the PSTN infrastructure.

BIPAC 7100SV extracts the maximum benefit from Voice over IP (VoIP) technology. It interfaces analog telephones with IP-based telephony networks. The integration of VoIP technology and ADSL Modem/Router is undoubtedly the most economic and practical solution to modern society.

1.2 Package Contents

1. Billion BIPAC 7100SV VoIP ADSL Modem/Router
2. One CD-ROM containing online manual
3. One Quick Start Guide
4. One RJ-11 ADSL/telephone cable
5. One CAT-5 straight LAN cable
6. One power adapter (12V DC 1.2A)

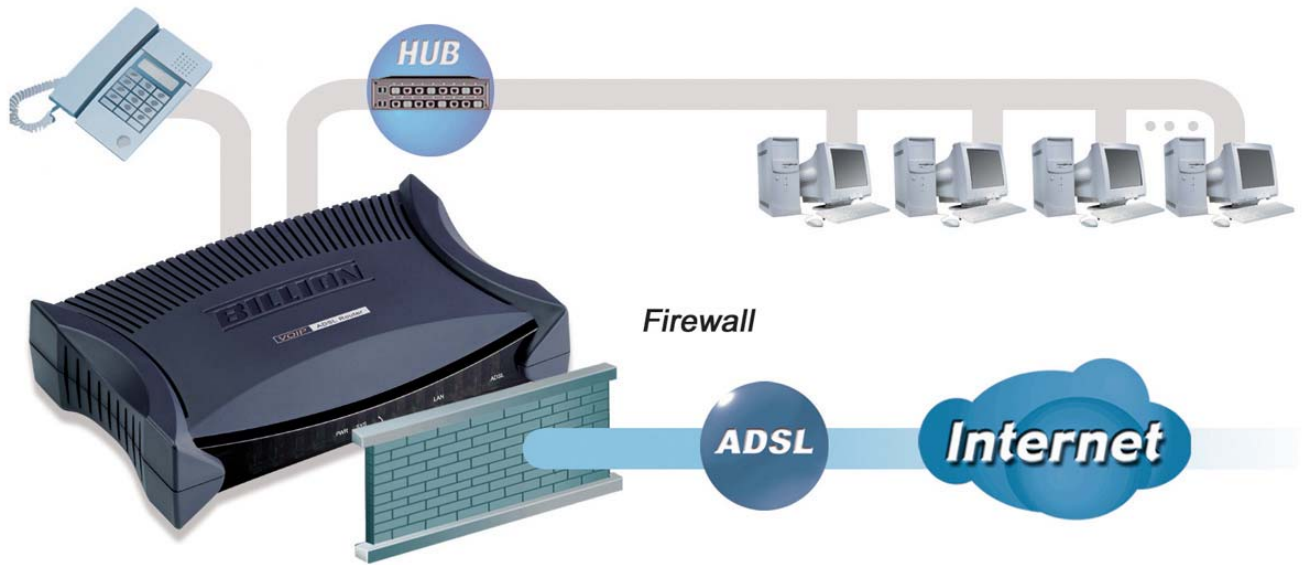
1.3 BIPAC 7100SV Features

BIPAC 7100SV ADSL Modem/Router provides the following features:

- **ADSL Multi-Mode Standard:** Supports downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2); G.hs (G994.1)).
- **Multi-Protocol to Establish A Connection:** Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) and IPoA (RFC1577) to establish a connection with ISP. The product also supports VC-based and LLC-based multiplexing.
- **Quick Installation Wizard:** Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the ISP, then surf the Internet immediately.
- **Universal Plug and Play (UPnP) and UPnP NAT Traversal:** This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.
- **Network Address Translation (NAT):** Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Ping and others.
- **Domain Name System (DNS) relay:** Provides an easy way to map the domain name (a friendly name for user such as www.yahoo.com) and IP address. When local machine sets its DNS server with this router's IP address. Then every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in outside network. After the router gets the reply, then forwards it back to the PC.

- **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply an account from this free Web server <http://www.dyndns.org/>. There are more than 5 DDNS servers supported.
- **PPP over Ethernet (PPPoE):** Provides embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer. The Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are provided, too.
- **Virtual Server:** User can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, user can assign a PC in LAN acting as WEB server inside and expose it to the outside network. Outside user can browse inside web server directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.
- **Firewall:** Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. Packet filtering is also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.
- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate multiple clients IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **Rich Packet Filtering:** Not only filter the packet based on IP address, but also based on Port numbers and MAC address. It will increase the performance in LAN and WAN, also provide a higher-level security control
- **SNTP:** An easy way to get the network real time information from an SNTP server.
- **Web based GUI:** Supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

1.4 BIPAC 7100SV Application



Using Billion VoIP ADSL Modem/Router

2.1 Cautions for Using Billion VoIP ADSL Modem/Router

Do not place the router under high humidity and high temperature.



Do not use the same power source for the device with other equipment.

Do not open or repair the case yourself. If the device is too hot, turn off the power immediately and have a qualified serviceman repair it.

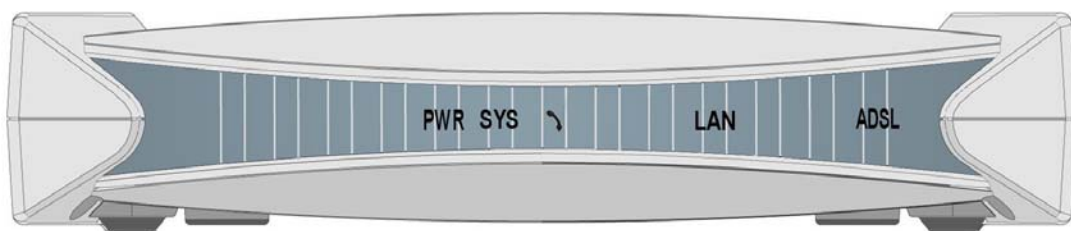
Avoid using this product and all accessories outdoors.



Place the product on the stable surface.

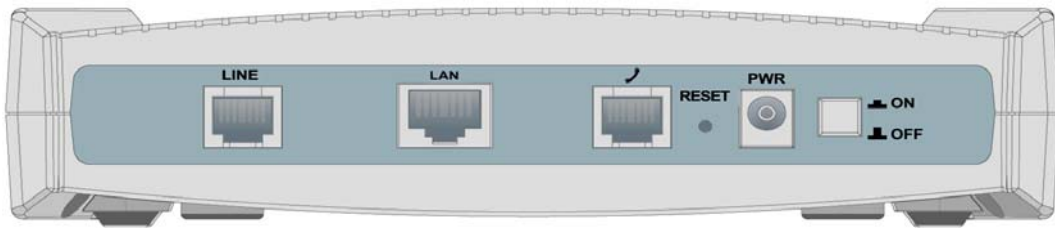
Only use the power adapter that comes with the package.

2.2 The Front LEDs



LED	Meaning
PWR	Lit green when power adapter is connected.
SYS	When flash, it indicates that the device is working properly.
Phone	Lit green when the phone is off hook.
LAN	Lit green when the LAN link is connected.
ADSL	When lit, it indicates that the ADSL (Line) port is connected to the DSLAM and working properly.

2.3 The Rear Ports



LED	Meaning
Power Switch	A Power ON/OFF switch
Power Jack	Connect the supplied power adapter to this jack.
Reset	Press it to restore the factory default setting back.
VoIP	Connect RJ-11 cable to this port when connecting to an analog phone set.
LAN (RJ-45 connector)	Connect the supplied Ethernet cable to this port when connecting to a NIC (Network Interface card) in PC. Connect an UTP Ethernet cable to this port when connecting to a LAN such as an office or home network.
LINE (RJ-11 connector)	Connect the supplied RJ-11 cable to this port when connecting to the ADSL

2.4 Cabling

The most common problem associated with Ethernet is bad cabling or ADSL line. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, please verify that the PWR, LAN and ADSL LEDs are lit and SYS LED is blinking. If they are not, verify that you are using the proper cables.

So long as the cables are connected and the LEDs are lit normally, follow **“Chapter 3 Configuration”** below to modify the network settings.

BIPAC 7100SV can be configured with your Web browser. The web browser is included as a standard application in following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me/XP, etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with BIPAC 7100SV, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to BIPAC 7100SV either directly or through a hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address which must be in the same subnet of BIPAC 7100SV. The default IP address of router is 192.168.1.254 and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from BIPAC 7100SV.

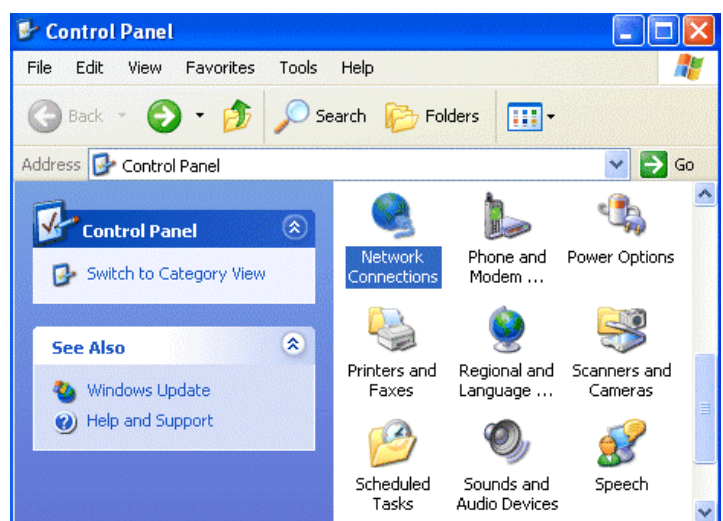
Please follow the steps below for PC's network environment installation. Before taking the first step, please check your PC's network components. If your PC connects the ADSL Modem/Router through Ethernet port, the TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows relative manuals.



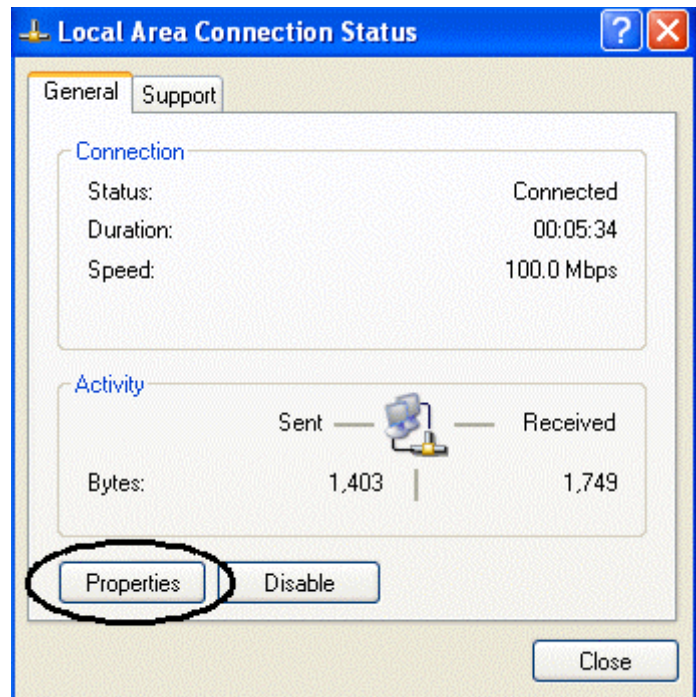
Any TCP/IP capable workstation can be used to communicate with or through BIPAC 7100SV. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC in Windows XP

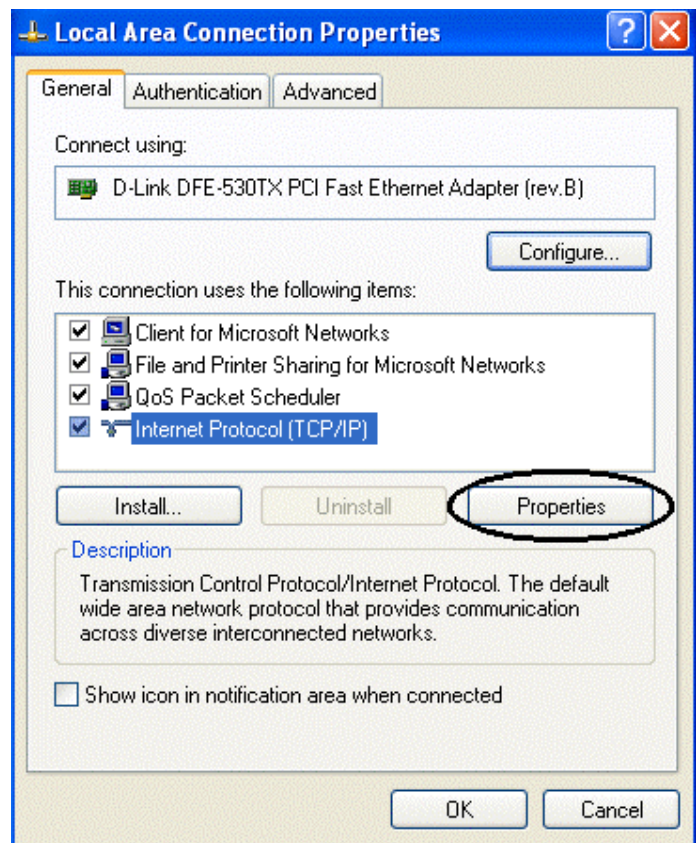
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**.



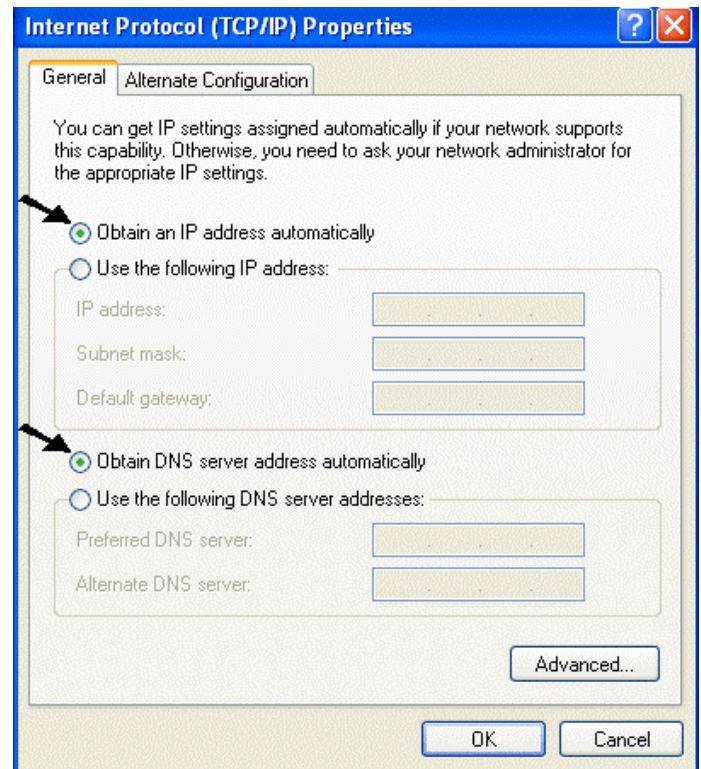
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

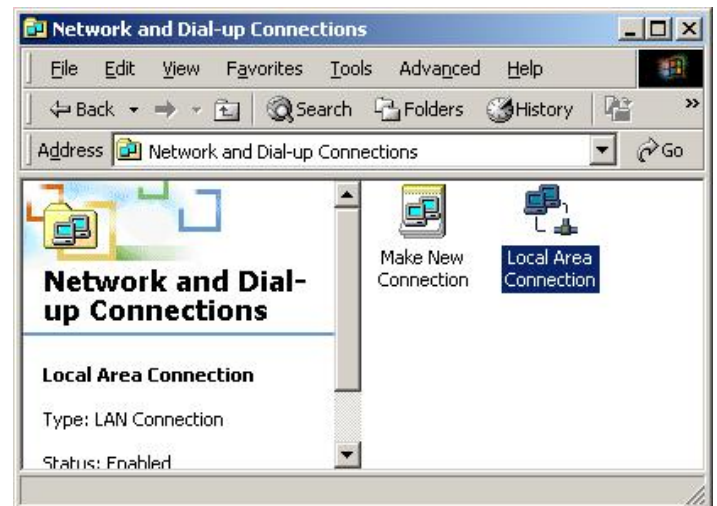


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

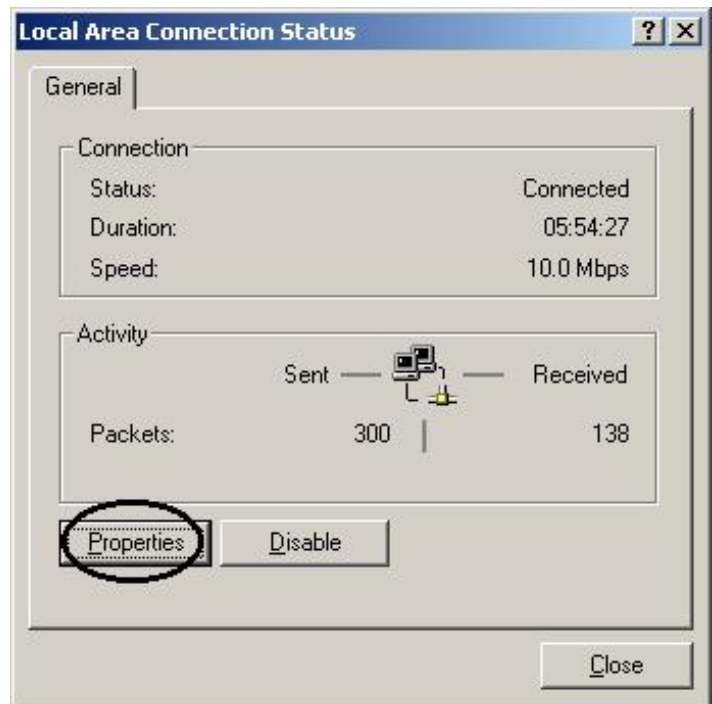


Configuring PC in Windows 2000

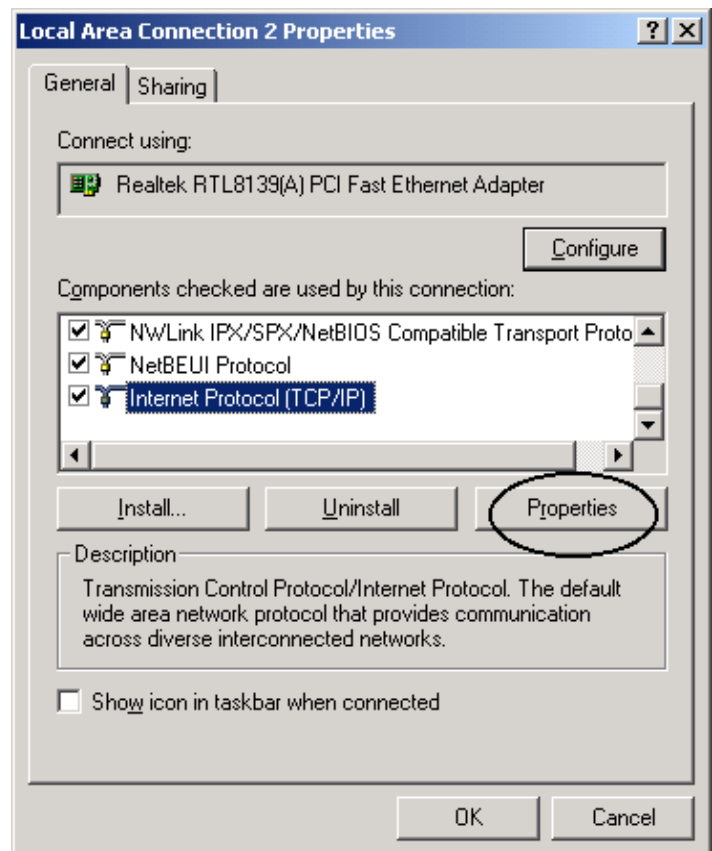
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.



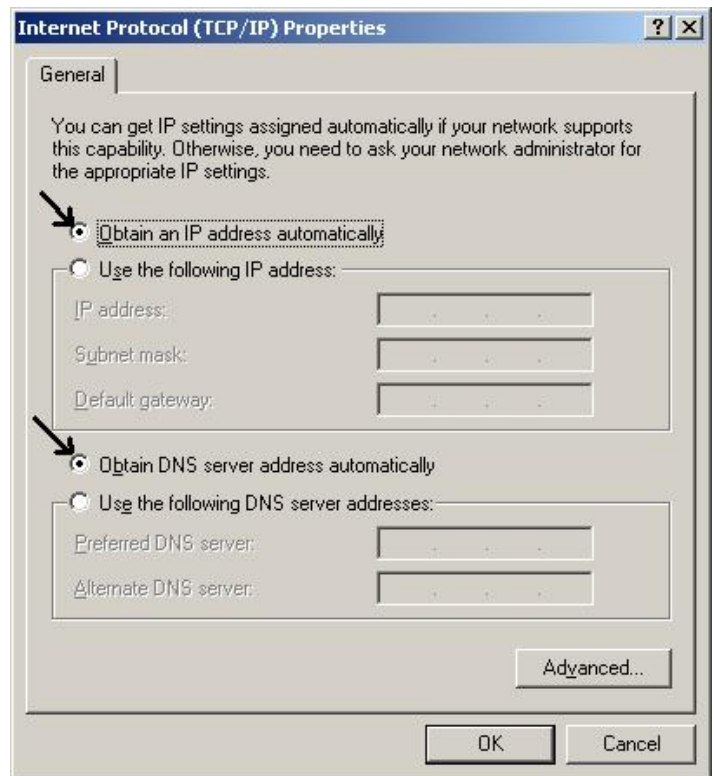
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

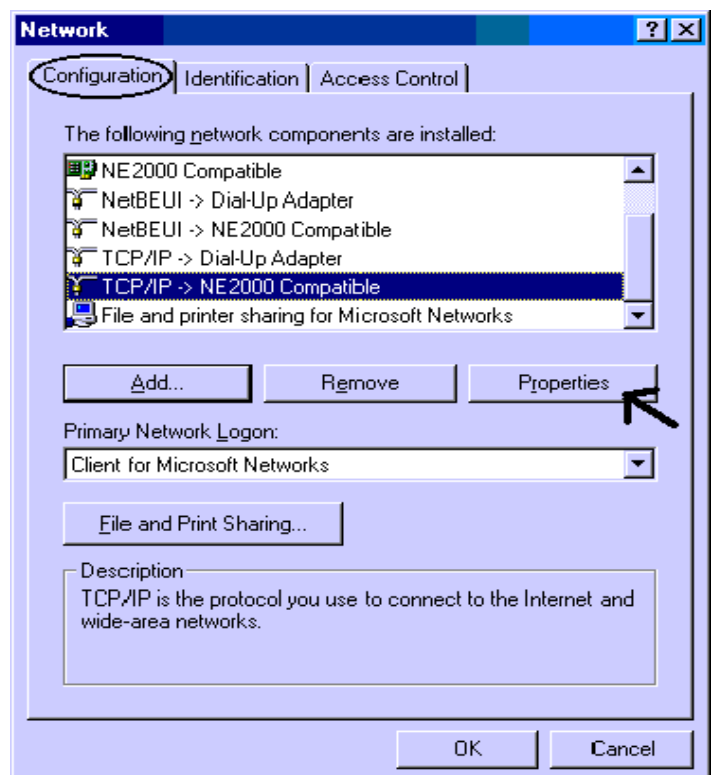


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

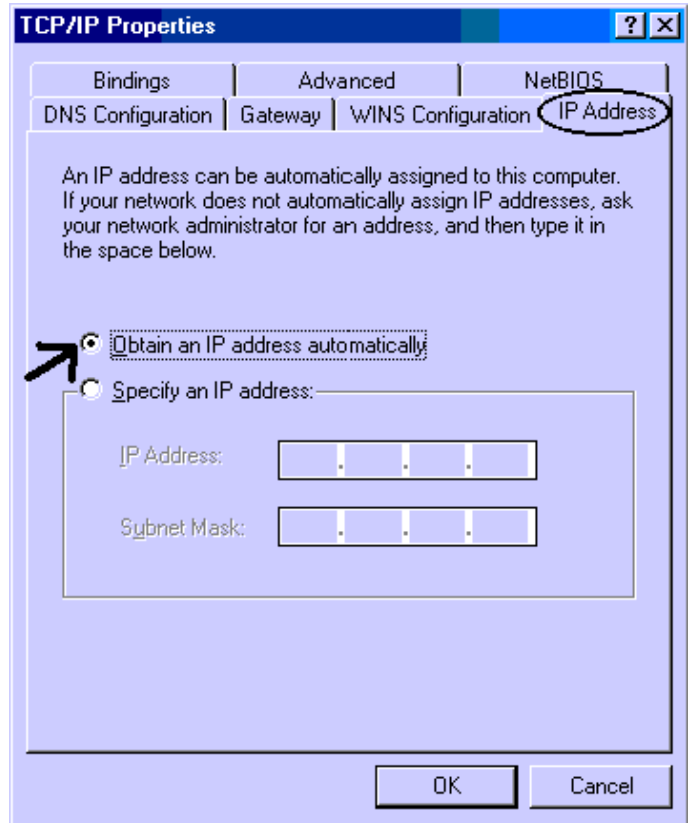


Configuring PC in Windows 95/98/ME

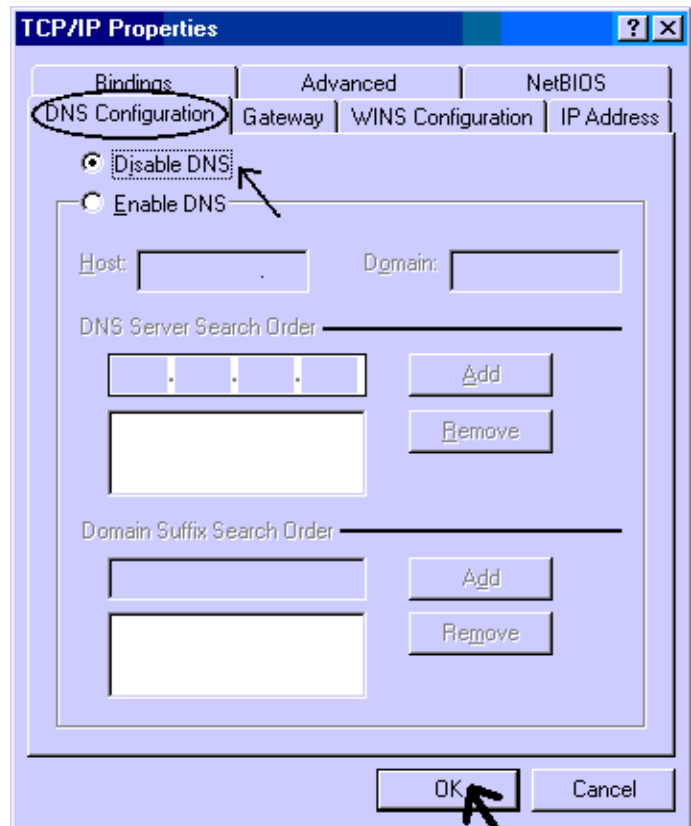
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Click **Properties**.



4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.

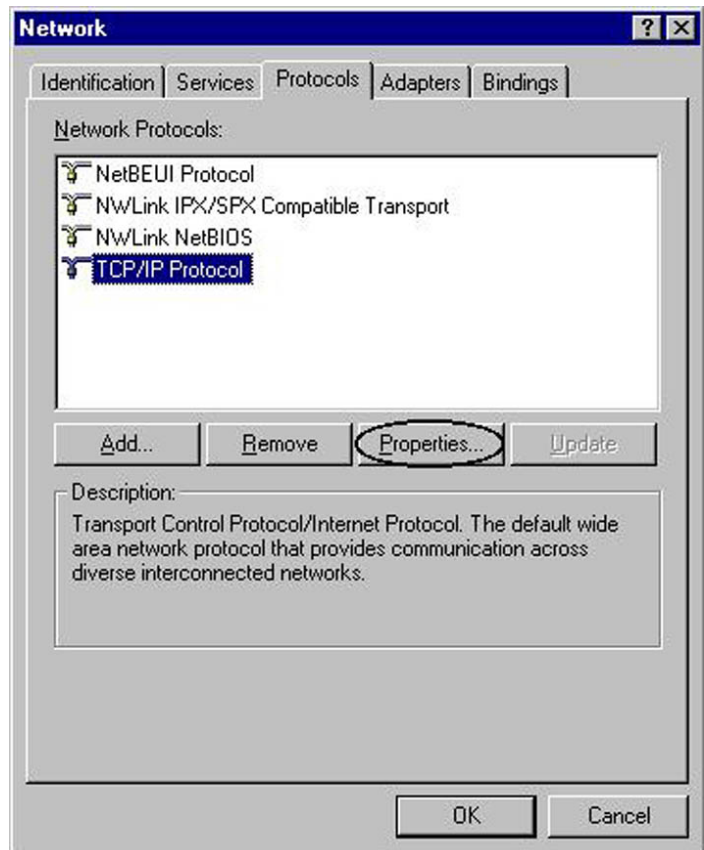


5. Then select the **DNS Configuration** tab.
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

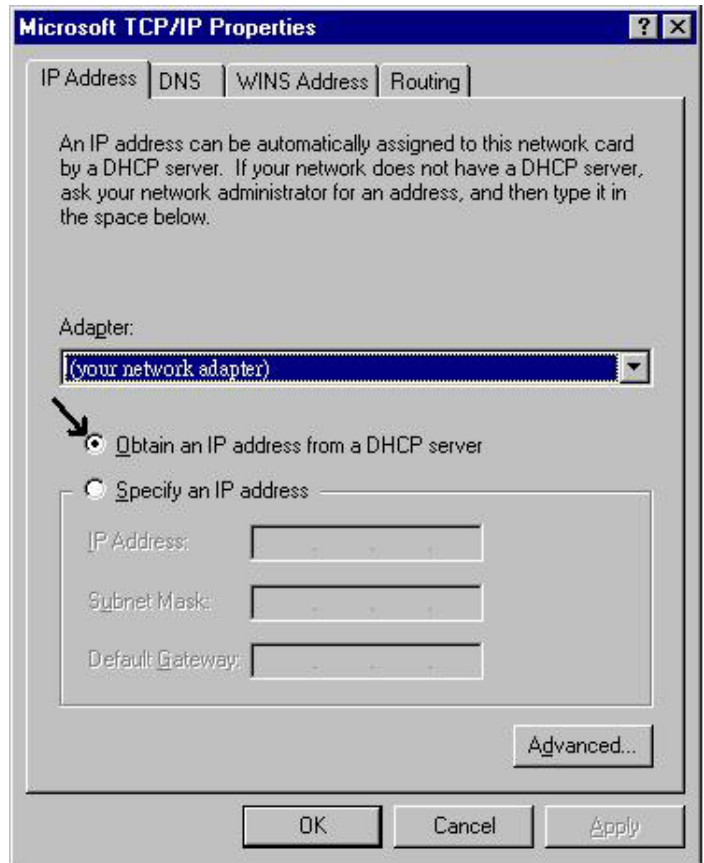


Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



3.2 Factory Default Settings

Before you configure this device, you need to know the following default settings.

1. Web Configuration

Password: There are two levels of password protection, **Administrator Level** and **User Level**.

	User Name	Password
Administrator Level	admin	password
User Level	user	password

2. Device IP Network settings in LAN site

IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

3. ISP setting in WAN site

Virtual Circuit 0: 1483 Routed IP LLC

4. DHCP server

DHCP server is enabled.
IP address pool from IP Address: 192.168.1.100 to IP Address: 192.168.1.199

3.2.1 Password

The default username and password are admin and password respectively.



If you ever forget the password to log in, you may press the RESET button up to 2 seconds to restore the factory default settings.

3.2.2 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	Obtain an IP address automatically. ISP assigns this IP address.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199 (Actually, it can supports up to 253 users.)	

3.3 Information from ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IPoA, or PPTP-to-PPPoA Relaying.

Gather the information as illustrated in the following table and keep it for reference.

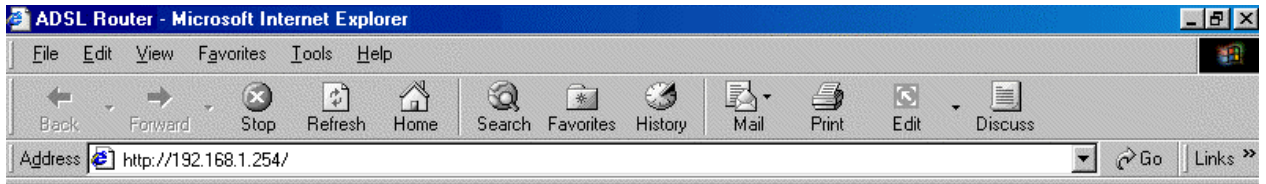
PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

IPoA	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
------	---

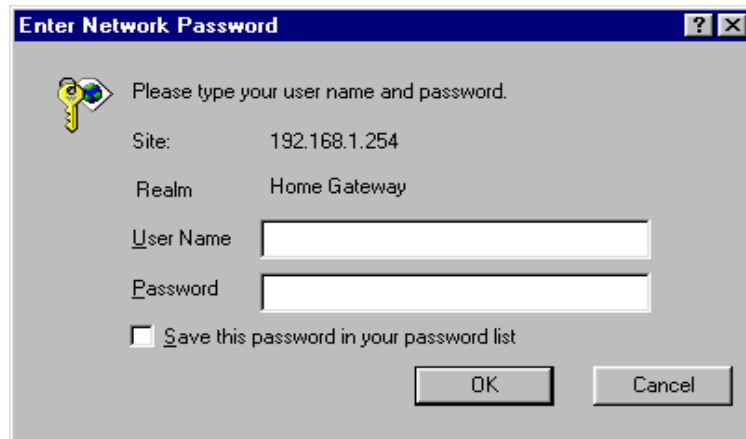
3.4 Configuring with Web Browser

The ADSL Modem/Router can be configured with your Web browser. The web browser is included as a standard application in following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me/XP, etc. The product provides a very easy and user-friendly interface for configuration.

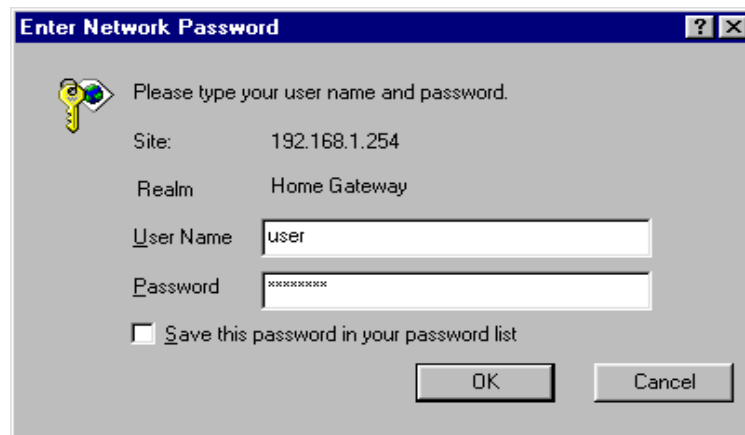
Open the web browser, enter the local port IP address of the ADSL Router, which default at **192.168.1.254**, and click “Go” to get the login page.



There are two levels of password protection. The first level is for administrator and the second one is for user.



If you want to configure the device with administrator level, type **admin** in the username field and **password** in the password field. Then, click “OK” to log in. You can modify these passwords for security and management purpose.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.254

Realm: Home Gateway

User Name: user

Password: *****

Save this password in your password list

OK Cancel

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status** (ADSL Status, LAN Status, PPP Status, Learned MAC Table, Routing Table, System Log, Security Log)
- **Quick Start**
- **Configuration** (WAN, LAN, VoIP, System, Firewall, Virtual Server, Advanced)

3.4.1 Status

The Status section provides and contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. It also provides useful information for users to review the status of device.

System Status

Device Info

Firmware Version:	CX82xxx_4.1.0.9_B214a
Customer Software Version:	4.1.0.9_BiB214a_1

WAN

IP Address	Subnet Mask	MAC Address
192.168.241.101	255.255.255.0	00:04:ED:00:07:71

LAN

IP Address	Subnet Mask	MAC Address
192.168.1.254	255.255.255.0	00:04:ED:00:07:70

DHCP Clients

	IP Address	MAC Address
1	192.168.1.123	00:0D:88:18:53:91

SAVE CONFIG RESTART

3.4.1.1 Status – ADSL Status

Displays the status of your ADSL connection. It will refresh every two seconds.

ADSL Status

Information

Showtime Firmware Version	3.30
Line State	ACTIVATION
Modulation	N/A
Annex Mode	ANNEX_A
Startup Attempts	0
Max Tx Power	-38 dBm/Hz
CO Vendor	UNUSED_VENDOR_0
Elapsed Time	0 days 0 hours 7 minutes 51 seconds

	Downstream	Upstream	
SNR Margin	NA	NA	dB
Line Attenuation	NA	NA	dB
Errored Seconds	0	0	
Loss of Signal	0	0	
Loss of Frame	0	0	
CRC Errors	0	0	

SAVE CONFIG RESTART

3.4.1.1.1 ADSL Status – WAN Status

WAN Status

Select Virtual Circuit

Virtual Circuit: 0
Release

Execute

Information

IP Address	Subnet Mask	MAC Address
192.168.241.101	255.255.255.0	00:04:ED:00:07:71

SAVE CONFIG RESTART

3.4.1.1.2 ADSL Status – ATM Status

ATM STATUS

Statistic

	Transmit	Receive
Bytes	0	0
Cells	0	0
HEC Errors	N/A	0
Mgmt Cells	0	0
CLP0 Cells	0	0
CLP1 Cells	0	0
Errors	0	0
Misrouted Cells	N/A	0

Reset Counters

SAVE CONFIG RESTART

3.4.1.2 Status – LAN Status

Displays the status of your Local Area Network (LAN) connection.

LAN Status		
Information		
IP Address	Subnet Mask	MAC Address
192.168.1.254	255.255.255.0	00:04:ED:00:07:70

SAVE CONFIG RESTART

3.4.1.2.1 LAN Status – TCP Status

TCP Status	
Statistic	
Total Packets Sent	2549
Data Packets Sent	1705
Data Bytes Sent	1194464
Total Packets Received	1994
Packets Received in-sequence	285
Bytes Received in-sequence	108919
Out of Order Packets	272
Out of Order Bytes	0
Packets disgarded for bad checksum	0
Packets disgarded for bad header offset	0
Packets disgarded because too short	0
Connections Initiated	0
Connections Accepted	285
Connections	285

SAVE CONFIG RESTART

3.4.1.3 Status- PPP Status

Displays the status of your PPP connection. It will refresh every ten seconds.

PPP Status

If a * appears under Mode column, you need to [check the WAN configuration](#) make sure the VC has the correct encapsulation.

Connection #

Information

#	Connection Name	Interface	Mode	Status	Pkts Sent	Pkts Rcvd	Bytes Sent	Bytes Rcvd
---	-----------------	-----------	------	--------	-----------	-----------	------------	------------

SAVE CONFIG RESTART

3.4.1.4 Status- Learned MAC Table

Aging Timeout: Enter the time period for the router to memorize MAC addresses.

Learned MAC Table	
Parameters	
Aging Timeout	100 Seconds
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	
Information	
MAC Address	Expiration
00:0D:88:18:53:91	100

3.4.1.5 Routing Table

Display the current routing paths of BIPAC 7100SV.

Routing Table			
Parameters			
Destination	Netmask	Gateway	Interface
192.168.1.0	255.255.255.0	192.168.1.254	br0
192.168.241.0	255.255.255.0	192.168.241.101	ss0
127.0.0.1	255.0.0.0	127.0.0.1	lo0

3.4.1.6 System Log

Display the system logs cumulated till the present time. You can trace the historical information through this function.

System Log

Current Time: THU JAN 01 00:20:01 1970

If you would like to save the log to a text file, right click [here](#) and select "Save Target As ..."

```

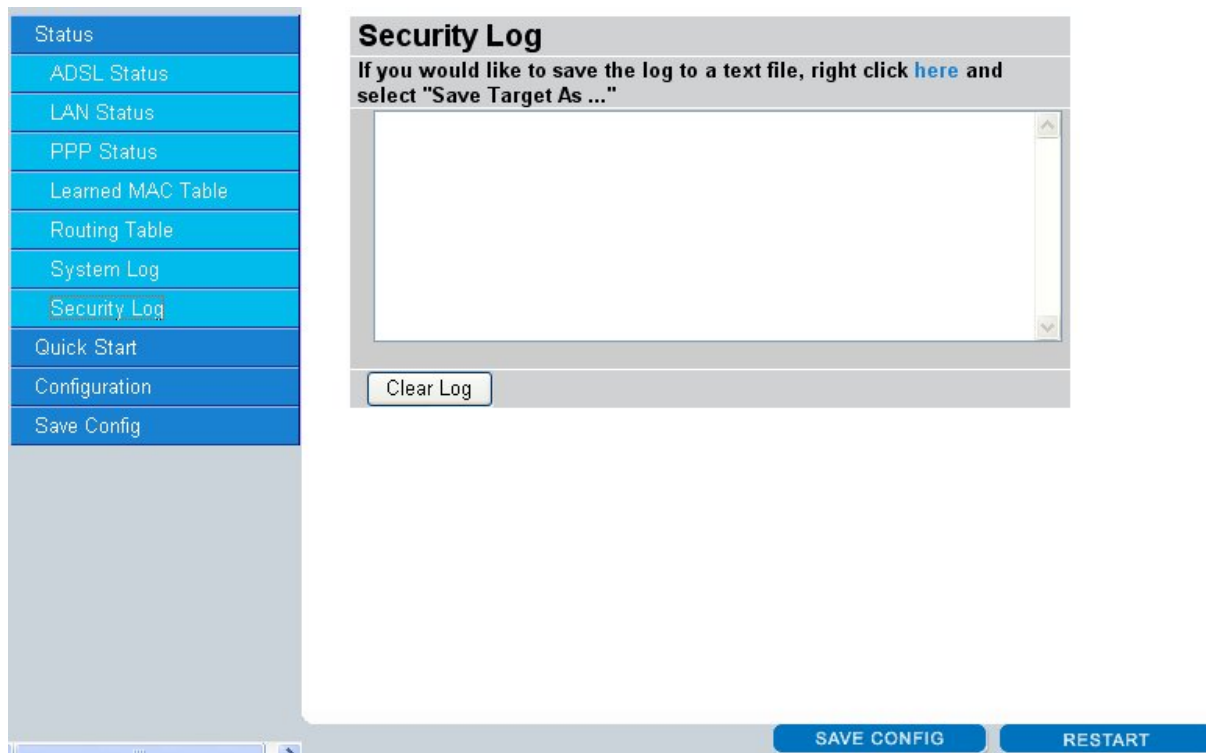
01/01/1970 00:00:00> CfgMgr: 'AtaApp.out' module loaded.
01/01/1970 00:00:00> CfgMgr: 'Washer.dlz' module loaded.
01/01/1970 00:00:00> No Static Session Information is
defined.
01/01/1970 00:00:00> NAT/NAPT Session Start: interface
ss0, WAN IP is 192.168.241.101
01/01/1970 00:00:00> CfgMgr: 'Shtm.dlz' module loaded.
01/01/1970 00:00:00> Initialized Dynamic NAPT.
01/01/1970 00:00:00> ATM: Setting up vcc0, VPI=0, VCI=32

```

Clear Log

3.4.1.7 Security Logs

Display the information of security logs. If hacker attacks your sever, he will be isolated by the firewall function and the router will record related information. Hence, you know where the hacker comes from.



3.4.2 Quick Start

If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router to access the Internet and enable VoIP service without a problem.

3.4.2.1 ADSL Quick Start

Please check **Chapter 3.3** (*Information from the ISP*), then enter the proper values into this web page, click the **Apply** button and then click the **Save Config** button to save all of the configuration parameters to FLASH. After the router reboot, you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.

Status
Quick Start
ADSL
VoIP
Configuration
Save Config

ADSL Quick Start

Pvc 0

Per VC Settings

Virtual Circuit: Enabled

Connection

Encapsulation: 1483 Bridged IP LLC

Bridge: Enabled

VPI: 0

VCI: 32

Static IP Settings

IP Address: 192.168.241.101

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Account Setup

Username:

Password:

Automatic Reconnect:

Submit Reset

SAVE CONFIG RESTART

3.4.2.2 VoIP Quick Start

If you have a VoIP SIP account, you may configure it to enable this service. Please refer to the sections (VoIP configuration) below for more information.

Status
Quick Start
ADSL
VoIP
Configuration
Save Config

VoIP Quick Start

SIP Parameters

SIP Registration: Enable Disable

Local SIP Port: 5060

Start Media Port (RTP): 5000

User ID: 89722

Password:

Service Provider Parameters

Service Provider: DEFAULT

Registrar Address: fwd.pulver.com

Registrar Port: 5060

Submit Reset

Note: The SIP Parameters fields should be changed when a different Service Provider is chosen.

SAVE CONFIG RESTART

3.4.3 Configuration

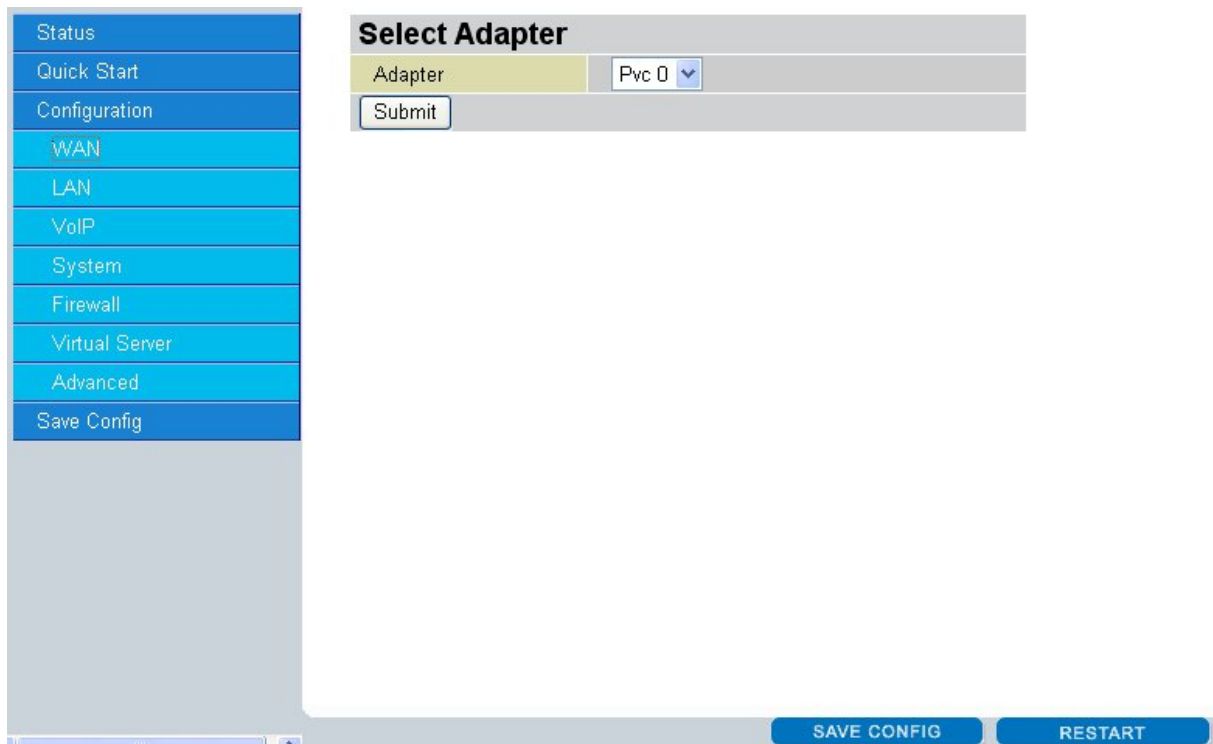
When you click this item, you get following sub-items to configure BIPAC 7100SV.

LAN, WAN, Firewall, System, VPN, Virtual Server, Advanced and Help

3.4.3.1 WAN

The screens below contain settings for the WAN interface toward Internet.

Select Adapter



Select the item of **PVCs** you want to configure. Then, press the **Submit** button.

Status	WAN Configuration	
Quick Start	Pvc 0 <input type="button" value="Change Adapter"/>	
Configuration	Virtual Circuit	
WAN	Virtual Circuit	Enabled <input type="button" value="v"/>
LAN	Bridge	Enabled <input type="button" value="v"/>
VoIP	IGMP	Disabled <input type="button" value="v"/>
System	Encapsulation	1483 Bridged IP LLC <input type="button" value="v"/>
Firewall	ATM	
Virtual Server	VPI	0
Advanced	VCI	32
Save Config	Service Category	UBR <input type="button" value="v"/>
	Peak Cell Rate	0 kbps
	Sustainable Cell Rate	0 kbps
	Max Burst Size	0
	DHCP Client	
	DHCP Client	Disabled <input type="button" value="v"/>
	Host Name	<input type="text"/>
	MAC Spoofing	
	MAC Spoofing	Disabled <input type="button" value="v"/>
	Mac Address	00:00:00:00:00:00
	Static IP Settings	
	IP Address	192.168.241.101
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	PPP	
	PPP	Advanced PPP configuration
	Service Name	<input type="text"/>
	Username	<input type="text"/>
	Password	<input type="text"/>
	Disconnect Timeout	0 minutes (Max:32767)
	MRU	1492
	MTU	1492
	MSS	1432
	Lcp Echo Interval	10 seconds
	Lcp Echo Maximum Consecutive Failure	6
	Authentication	Auto <input type="button" value="v"/>
	Automatic Reconnect	<input type="checkbox"/> PPP Disconnect Timer Config
	<input type="button" value="Submit"/>	<input type="button" value="Reset"/>
	<input type="button" value="SAVE CONFIG"/> <input type="button" value="RESTART"/>	

Virtual Circuit

Virtual Circuit: Enable/Disable the settings of this VC.

Bridge: If you set this device to be bridge mode, select Enable; if not, please select Disable.

IGMP: You can Enable or Disable this function.

Encapsulation: There are eleven ways — PPPoE VC-Mux, PPPoE LLC, PPPoE None, PPPoA VC-Mux, PPPoA LLC, 1483 Bridged IP VC-Mux, 1483 Bridged IP LLC, 1483 Routed IP VC-Mux, 1483 Routed IP LLC, Classical IP over ATM, Native ATM — for the device to have a public IP address and then to access Internet. You have to check with your ISP about which way is adopted. **VPI:** Consult the telephone company to get the Virtual Path Identifier (VPI) number. The default value is 0.

ATM

VPI: Consult the telephone company to get the Virtual Path Identifier (VPI) number. The default value is 0.

VCI: Consult the telephone company to get the Virtual Channel Identifier (VCI) number. The default value is 32.

Service Category: Select **UBR** or **CBR**.

DHCP Client

DHCP Client: Check to enable the DHCP client function if you want the device to get an IP address automatically from your ISP.

Host Name: Enter the name of your work group.

MAC Spoofing

MAC Spoofing: The MAC Spoofing is for solving the scenario when the ISP only recognizing the specified MAC address.

Static IP Settings

IP Address: Enter the information provided by your ISP.

Subnet Mask: Enter the information provided by your ISP.

Default Gateway: Enter the gateway address provided by your ISP.

PPP

If your encapsulation is set to be PPPoE or PPPoA, the following fields must be entered.

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is 31 alphanumeric characters.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Disconnect Timeout **seconds:** Auto-disconnect the ADSL Router when there is no activity on the line for a predetermined period of time. You can input any number from 0 to 32767. The default value is 0 seconds.

MRU: Maximum Receive Unit indicates the peer of PPP connection the maximum size of the PPP information field this device can be received. The default value is 1492 and is used in the beginning of the PPP negotiation. In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MTU: Maximum Transmission Unit indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU. The default value is 1492.

MSS: Maximum Segment Size is the largest size of data that TCP will send in a single IP packet. When a connection is established between LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their MSS during the TCP connection handshake. The default value is 1492.

Authentication: Default at "Auto".

Automatic Reconnect: Check to enable this device to automatically re-establish the PPPoE session when disconnected by ISP.

3.4.3.2 LAN

This screen contains settings for LAN interface attached to the LAN port.

Device IP Address

IP Address: Default at 192.168.1.254.

This is the device IP address in LAN site. If you plan to change it to another IP address to a different range of IP subnet. Please make sure your PC is also located at the same IP subnet. Otherwise, you may not be able to access the router.

Subnet Mask: Default at 255.255.255.0.

DHCP Server

DHCP Server: Check DHCP Server to enable the router to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated. If you do not check this selection, remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful not to assign the same IP address to different computers.

DHCP address pool selection: Auto or User Defined. If select the AUTO, router will assign an IP address back to PC's IP request. If User Defined, please specify the IP pool range.

User Defined Start Address: Enter the start address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is 192.168.1.100.

User Defined End Address: Enter the last address of this local IP network address pool that you want the DHCP server to assign IP addresses to. The default value is 192.168.1.199.

With this case, the DHCP pool is from 192.168.1.100 to 192.168.1.199. Therefore, the local computer will get an IP address located at this range randomly.

Lease Time: Set the lease time you required.

User Mode: There are two selections, Single User and Multi-User, for this setting.

3.4.3.3 VoIP

The screens below contain settings for the VoIP module. This will create the telephone like service in the Internet. Most of VoIP services are free when surfing in the Internet.

VoIP	
ATAA Software Version:	ATAApp 1.00.10
PTM Software Version:	2.33.06_RC built on May 31 2004, 17:03:43

At the bottom of the interface, there are two buttons: **SAVE CONFIG** and **RESTART**.

VoIP: Enable/Disable the settings of VoIP module

3.4.3.3.1 Configuration

This screen contains settings for configuring VoIP SIP module.

Configuration	
SIP Parameters	
SIP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SIP Registration	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local SIP Port	5060
Start Media Port (RTP)	5000
User ID	89722
Password	*****
Authorization User ID	89722
Display Name	Conexant Ataa
Service Provider	DEFAULT
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Note: The SIP Parameters fields should be changed when a different Service Provider is chosen.

SIP: Enable/Disable to use SIP as VoIP call signaling protocol.

SIP Registration: Enable/Disable to register a SIP account in the SIP server (refer Service Provider section below) or not.

LocalSIPPort: Enter the local SIP port which device listens incoming request. (range from 5000 to 65535, default value is 5060)

MediaBasePort: It is known as RTP port, provide the based value from the media (RTP) ports that are assigned for various endpoints and the different call sessions that may exist within an end-point. (range from 5000 to 65535, default value is 5000)

UserID: This parameter holds the registration ID of the user within the SIP registrar.

Password: This parameter holds the password used for authentication within SIP registrar.

AuthorizationUserID: Same as UserID.

DisplayName: This parameter will be appeared on the Caller ID.

G.711U: Set the priority of voice compression to be used in the voice codec. Priority 1 owns the first priority and so on.

G.711A: Set the priority of voice compression to be used in the voice codec.

G.729A: Set the priority of voice compression to be used in the voice codec.

Please be noted. Then codec priority is selected using a drop-down box. If two codec type are assigned the same priority, then the priority is assigned in the order as G.711U > G.711A > G.729A in the decreasing order or priority. For example if the user selects 1, 2, 2 for G.711U, G.711A, and G.729A respectively, the application will assign priority as 1, 2, 3 for G.711U, G.711A and G.729A respectively.

3.4.3.3.2 Service Provider

This screen contains settings for register to get VoIP service from SIP service provider.

SIP Service Provider Configuration	
Parameters	
Working Service Provider	DEFAULT
New Service Provider	
Registration Interval	30 seconds
Authentication Method	AUTH_MD5
Registrar Address	fwd.pulver.com
Registrar Port	5060
Proxy Address	fwd.pulver.com
Proxy Port	5060
Outbound Proxy Address	fwd.pulver.com
Outbound Proxy Port	5060
Service Provide Action: List Current Service Provider Rules	
Submit Reset	

SAVE CONFIG RESTART

Registration Interval: specify the re-registration interval in seconds.

Authentication Method: specify the authentication method, currently MD5 is supported only.

Registrar Address: indicate the SIP registrar IP address

RegistrarPort: specify the port of the SIP registrar on which it will listen for register requests from VoIP device.

ProxyAddress: indicate the SIP proxy server IP address.

ProxyPort: specify the port of the SIP proxy server on which it will listen for messages.

OutbondProxyAddress: indicate the SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT.

OutbondProxyPort: specify the port of the SIP outbound proxy on which it will listen for messages.

3.4.3.3.3 Phone Book

This screen contains settings for creating phone book for speed dial. You can dial the “#0” to inform VoIP device to dial the VoIP number in the entry 0 of phone book.

Speed Dial	Abstract Description	Remote UserID	IP Address / Domain
#0			
#1			
#2			
#3			
#4			
#5			
#6			
#7			
#8			
#9			

Speed Dial: There are ten entries from 0 to 9. When you dial “#0” mapping to entry 0 in the phone book.

Abstract Description: indicate the purpose or useful information for this entry.

Remote UserID: This is the UserID you want to contact. Refer UserID in VoIP -> Configuration -> UserID.

IP Address / Domain: indicate remote user’s IP address or domain name if this remote user does not register in the SIP server. If remote user is registered in the SIP server, this field is related to the SIP server’s IP / Domain name.

For examples:

If your friend Tim gives you a SIP URL as sip:89755@192.246.69.223 then you can enter the Phone book as: Remote UserID: 89755

IP Address / Domain: 192.246.69.223

If your friend Felix gives you a SIP URL as sip:felix@iptel.org then you can enter the Phone book as:

Remote UserID: felix

IP Address / Domain: iptel.org

If your friend Greg gives you an IP address "192.246.56.56" only, then you can enter the Phone book as:

Remote UserID: (leave blank, don't fill anything)

IP Address / Domain: 192.246.56.56

3.4.3.3.4 Dial Plan

The screenshot displays the web interface of the Billion BIPAC 7100SV VoIP ADSL Router. On the left is a vertical navigation menu with the following items: Status, Quick Start, Configuration, WAN, LAN, VoIP, Configuration, Service Provider, Phone Book, Dial Plan, Call Feature, PTM, Ring Tone, Timer, System, Firewall, Virtual Server, Advanced, and Save Config. The 'Dial Plan' item is highlighted. The main content area is titled 'Dial Plan Configuration' and contains a 'Parameters' section with the following fields:

Parameters	
Working Service Provider	DEFAULT ▾
Rule Number	0
Prefix	
Prefix Timer	0 msecs
Not Allowed First Digits	
Long_NumDigits	0
Long_Timer	0 msecs
Short_NumDigits	0
Short_Timer	0 msecs
Suffix	
Dial Plan Action	DP_CALL ▾
Dial Plan Rule Action	Add New Rule ▾

Below the parameters are 'Submit' and 'Reset' buttons. At the bottom of the interface are 'SAVE CONFIG' and 'RESTART' buttons.

3.4.3.3.5 Call Feature

This screen contains settings for configuring the call feature.

Status	<h3>Call Feature Configuration</h3> <p>Parameters</p> <table border="1"> <tr> <td>Call Forwarding</td> <td><input type="checkbox"/> CallForwarding Unconditionally</td> </tr> <tr> <td></td> <td><input type="checkbox"/> CallForwarding On Busy</td> </tr> <tr> <td></td> <td><input type="checkbox"/> CallForwarding On No Ans</td> </tr> <tr> <td>Call Forwarding Number</td> <td><input type="text" value="79595"/></td> </tr> <tr> <td>Call Waiting</td> <td><input checked="" type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td>Call Return</td> <td><input checked="" type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td colspan="2"><input type="button" value="Submit"/></td> </tr> </table>	Call Forwarding	<input type="checkbox"/> CallForwarding Unconditionally		<input type="checkbox"/> CallForwarding On Busy		<input type="checkbox"/> CallForwarding On No Ans	Call Forwarding Number	<input type="text" value="79595"/>	Call Waiting	<input checked="" type="radio"/> Yes <input type="radio"/> No	Call Return	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input type="button" value="Submit"/>	
Call Forwarding		<input type="checkbox"/> CallForwarding Unconditionally													
		<input type="checkbox"/> CallForwarding On Busy													
		<input type="checkbox"/> CallForwarding On No Ans													
Call Forwarding Number		<input type="text" value="79595"/>													
Call Waiting		<input checked="" type="radio"/> Yes <input type="radio"/> No													
Call Return		<input checked="" type="radio"/> Yes <input type="radio"/> No													
<input type="button" value="Submit"/>															
Quick Start															
Configuration															
WAN															
LAN															
VoIP															
Configuration															
Service Provider															
Phone Book															
Dial Plan															
Call Feature															
PTM															
Ring Tone															
Timer															
System															
Firewall															
Virtual Server															
Advanced															
Save Config															

CallForwarding:

Check CallForwarding Unconditionally: VoIP device will forward all incoming call to the forwarding number.

Check CallForwarding On Busy: VoIP device will forward all incoming call to the forwarding number when user is already on the phone talking to someone.

Check CallForwarding On No Answer: VoIP device will forward all incoming call to the forwarding number when user is unavailable to pick up the phone.

CallForwardingNumber: specify the number to be used when user enable any type of call forwarding.

CallWaiting: Enable/Disable the call waiting feature.

CallReturn: Enable/Disable the call return feature.

3.4.3.3.6 PTM

PTM Configuration

Configure Caller ID Info

Modulation	CID_BELL202
Delay	550 msecs
FSK AMP 0	4096
FSK AMP 1	4096

Configure VAD

VAD

Disable VAD
 Enable VAD with Comfort Noise
 Enable VAD with Standard SID
 Enable VAD and Suppress SID

Configure Echo Cancellation

Enable Echo Cancellation Yes No

Configure DTMF Relay

DTMF Relay None (In Audio) RFC 2833

Configure Hook Flash Time

Hook Flash Max Time	1000 msecs
---------------------	------------

Configure Debounce Time

Debounce On-Off Time	300 msecs
----------------------	-----------

SAVE CONFIG RESTART

3.4.3.3.6 Ring Tone

This screen contains settings for creating different ring tone patterns.

Ring tone Configuration

Country Specific Ring Tone

Working Country	USA
New Country	

Ring Parameters

Ring Parameters	25,2000,4000,0,0
-----------------	------------------

Tone Parameters

Dial Tone	350,440,1000,0,0,0
Busy Tone	480,620,500,500,0,0
RingBack Tone	440,480,2000,4000,0,0
CallWaiting Tone	440,440,300,10000,0,0
Alerting Tone	350,0,100,100,100,100
Congestion Tone	480,620,250,250,0,0
Recall Tone	350,440,1000,0,100
Stutter Dial Tone	350,440,1000,0,100

Ring Tone Action Country

Submit Reset

SAVE CONFIG RESTART

Working Country: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically displayed. Current supported countries are USA and UK. New country can be added and defined by user

New Country: a text-field where you can enter the new country to add or modify some existing string. Please also refer below about Ring Tone Action to add, display, edit, or delete.

RingParameters: Defined by five fields, Frequency, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

DialTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

BusyTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

RingBackTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

CallWaitingTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

AlertingTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

CongestionTone: Defined by six fields, Frequency1, Frequency2, On Time1, Off Time1, On Time2, Off Time2. Frequency is given in hertz. Time is given in milliseconds.

RecallTone: Defined by five fields, Frequency1, Frequency2, On Time1, Off Time1, Duration. Frequency is given in hertz. Time and Duration are given in milliseconds.

StutterDialTone: Defined by five fields, Frequency1, Frequency2, On Time1, Off Time1, Duration. Frequency is given in hertz. Time and Duration are given in milliseconds.

Ring Tone Action: a drop-down selection (**Display, Add, Edit, Delete**)

Display -> display the selected country in the working country field after clicking submit button.

Add -> add a new country after clicking submit button according to the value that appears in the New Country field. This field must not be empty.

Edit -> rewrite the selected country (**working country** field) with current parameters after clicking submit button. The New Country field is optional and need to be filled only when the country code also has to be changed.

Delete -> delete the selected country (**working country** field) from the country list.

3.4.3.3.7 Timer

This screen contains settings for timers (all are given in seconds) in system level.

Timer Configuration		
Parameters		
Predial Timer	<input type="text" value="16"/>	seconds
Alert Timer	<input type="text" value="60"/>	seconds
Disconnect Timer	<input type="text" value="10"/>	seconds
RingBack Timer	<input type="text" value="60"/>	seconds
CallProgress Timer	<input type="text" value="60"/>	seconds
CallWaiting Timer	<input type="text" value="40"/>	seconds
CallFwdNoAns Timer	<input type="text" value="30"/>	seconds

Submit Reset

SAVE CONFIG RESTART

RedialTimer: indicate the time period through which the dial tone is heard once the phone is lifted off the hook. At the end of this period, if no digits have been pressed, VoIP device will start playing fast-busy tone.

AlertTimer: indicate the time for which VoIP device will play the ring when an incoming call has arrived and phone is on-hook. After this time period, the VoIP device will stop the ring automatically and reject the incoming call.

DisconnectTimer: indicate the time for which the fast-busy tone is played once a call has been disconnected by remote end. At the end of this time, the Warble tone will be played until the user hangs up the phone.

RingBackTimer: Indicate the time period for which the VoIP device will wait while the ring back tone is been played for the final response from the other end point once an outgoing call has been made and the initial response has been received.

CallProgressTimer: indicate the time period for which VoIP device will wait for initial response from the other end point once an outgoing call has been made.

CallWaitingTimer: indicate the time period for which the call-waiting tone will be played when an incoming call arrives in the connected state.

CallFwdNoAnsTimer: indicate the time period for which the call will be forwarded when no answered by anyone. This timer is applicable when “call forward on no answer” is enabled.

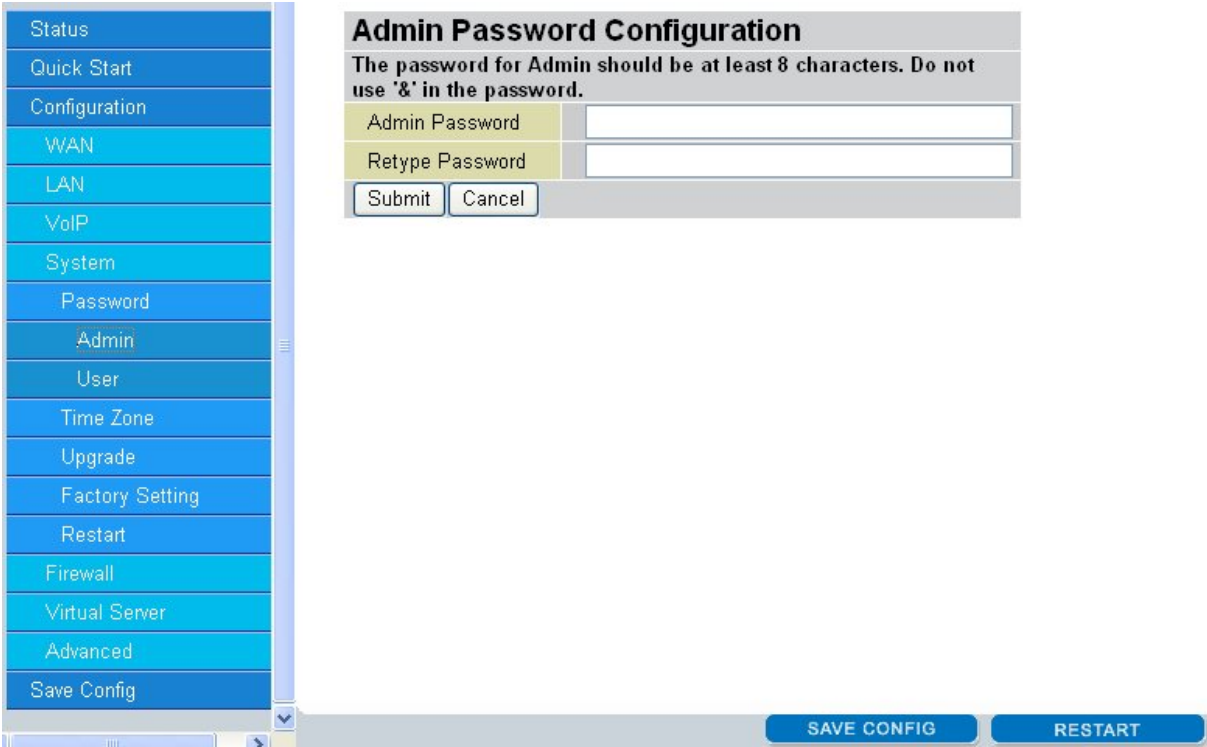
3.4.3.4 System

There are five items under the **System** section: Password, Time Zone, Upgrade, Factory Setting and Restart.

3.4.3.4.1 Password

In factory setting, the default password is **password**, and that for user is also password. You can change the default password to ensure that someone cannot adjust your settings without your permission. Every time you change your password, please record the password and keep it at a safe place.

Please note that the minimum input for password is **8** alphanumeric characters long. Since it is **case sensitive**, be sure that you remember whether a letter is in upper or lower case and make sure that your Caps Lock is off. Moreover, please do not use the sign “&” in the passwords.



The screenshot shows the 'User Password Configuration' page. On the left is a vertical navigation menu with items: Status, Quick Start, Configuration, WAN, LAN, VoIP, System, Password, Admin, User, Time Zone, Upgrade, Factory Setting, Restart, Firewall, Virtual Server, Advanced, and Save Config. The main content area has a title 'User Password Configuration' and a warning: 'Do not use '&' in the password.' Below this are two input fields: 'User Password' and 'Retype Password'. At the bottom of the form are 'Submit' and 'Reset' buttons. At the bottom right of the page are 'SAVE CONFIG' and 'RESTART' buttons.

3.4.3.4.2 Time Zone

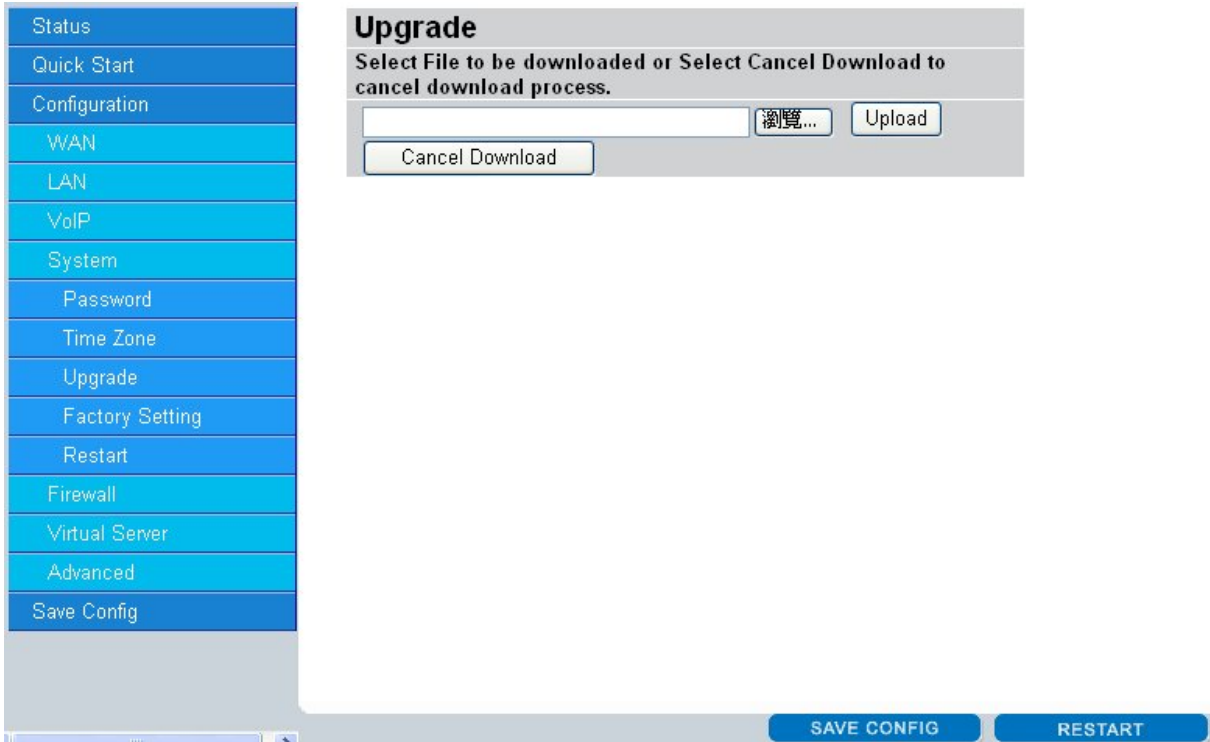
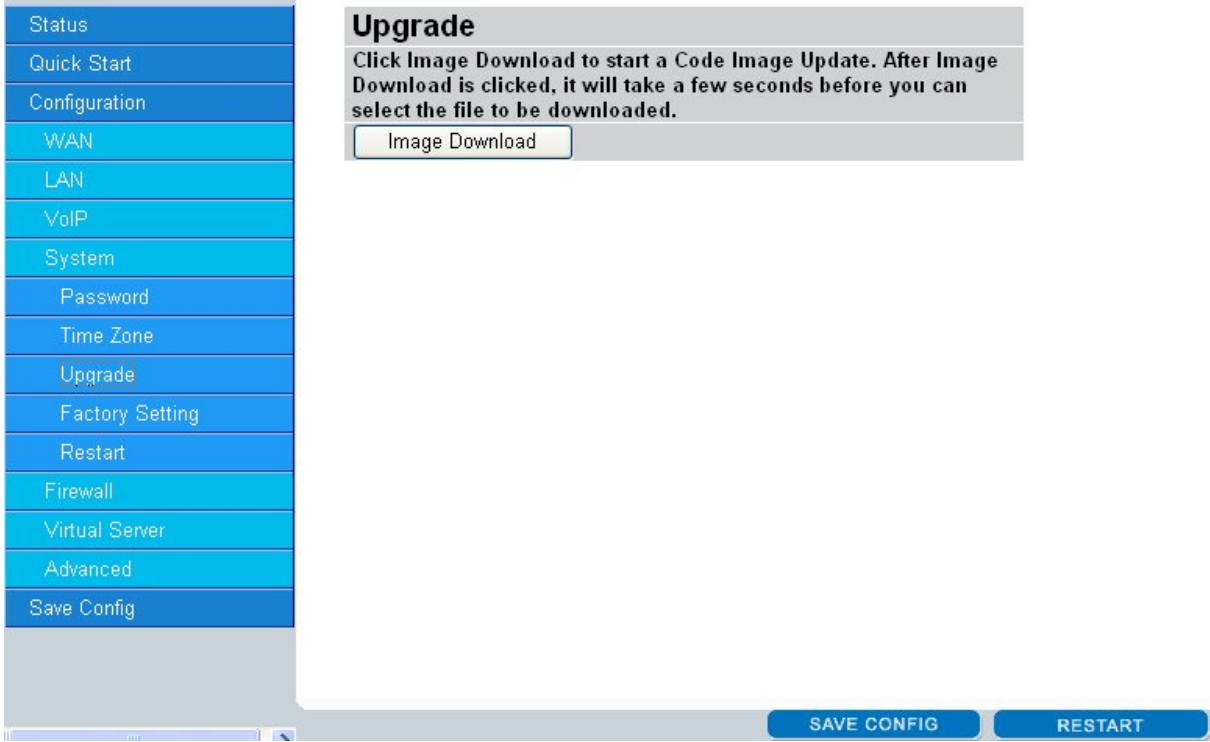
BIPAC 7100SV does not have a real time clock on board; instead, it uses the simple network time protocol (SNTP) to get the current time from the SNTP server in outside network. Please choose your local time zone and click Submit. You will get the correct time information after you really establish a connection to Internet. The current time of selected time zone will be shown in the Status – System window.

The screenshot shows the 'Time Zone' configuration page. The left navigation menu is the same as in the previous screenshot. The main content area has a title 'Time Zone' and a section 'Choose your local time zone' with a checked checkbox 'Automatically adjust clock for daylight saving changes'. Below this is a dropdown menu for 'Time Zone' showing '(GMT+01:00) Brussels, Copenhagen, Madrid, Paris, Vilnius'. There are input fields for 'SNTP Server IP Address' and 'Resync Poll Interval' (set to 30 minutes), with a 'Sync Now !' button. At the bottom of the form are 'Submit' and 'Cancel' buttons. At the bottom right of the page are 'SAVE CONFIG' and 'RESTART' buttons.

Automatically adjust clock for daylight saving changes: It is optional for different time zone area.

SNTP Server IP Address: Specify the IP address if you want to use your familiar SNTP server.

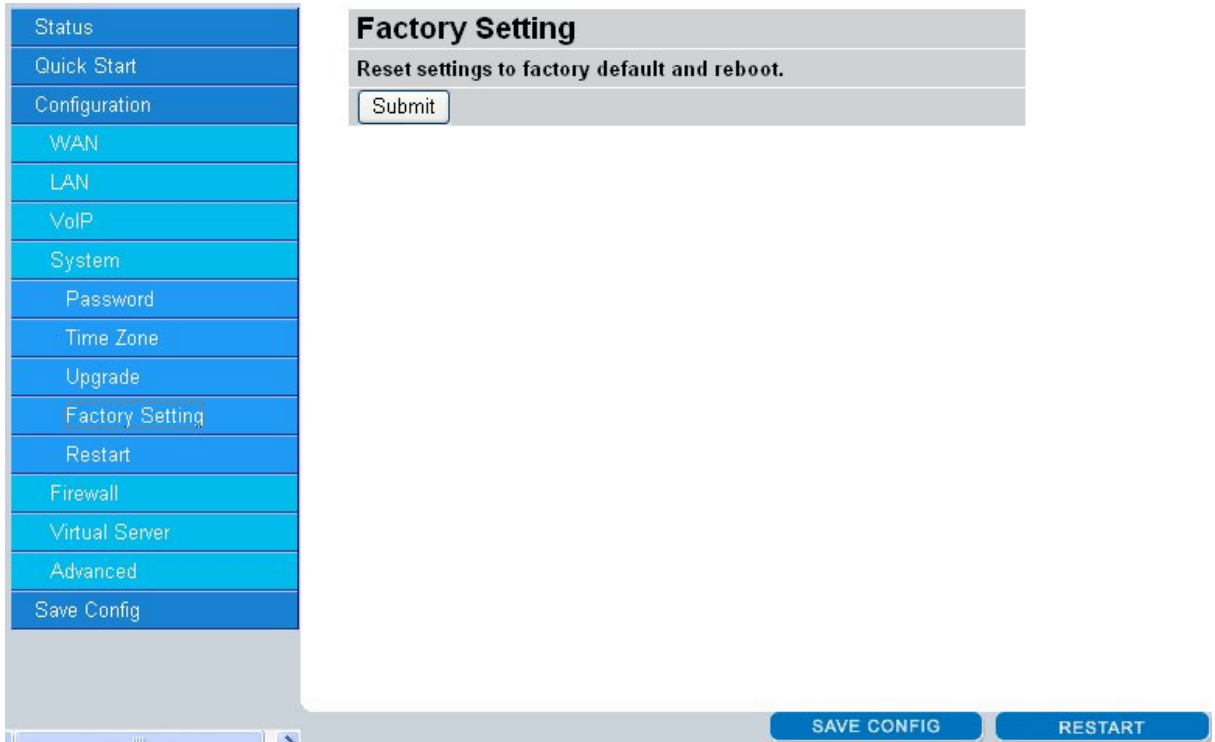
3.4.3.4.3 Upgrade



To upgrade the firmware of BIPAC 7100SV, you should download or copy the firmware to your local environment first. Press the “**Browse...**” button to specify the path of the firmware file. Then, click “**Upgrade**” to start upgrading. When the procedure is completed, BIPAC 7100SV will reset automatically to make the new firmware work.

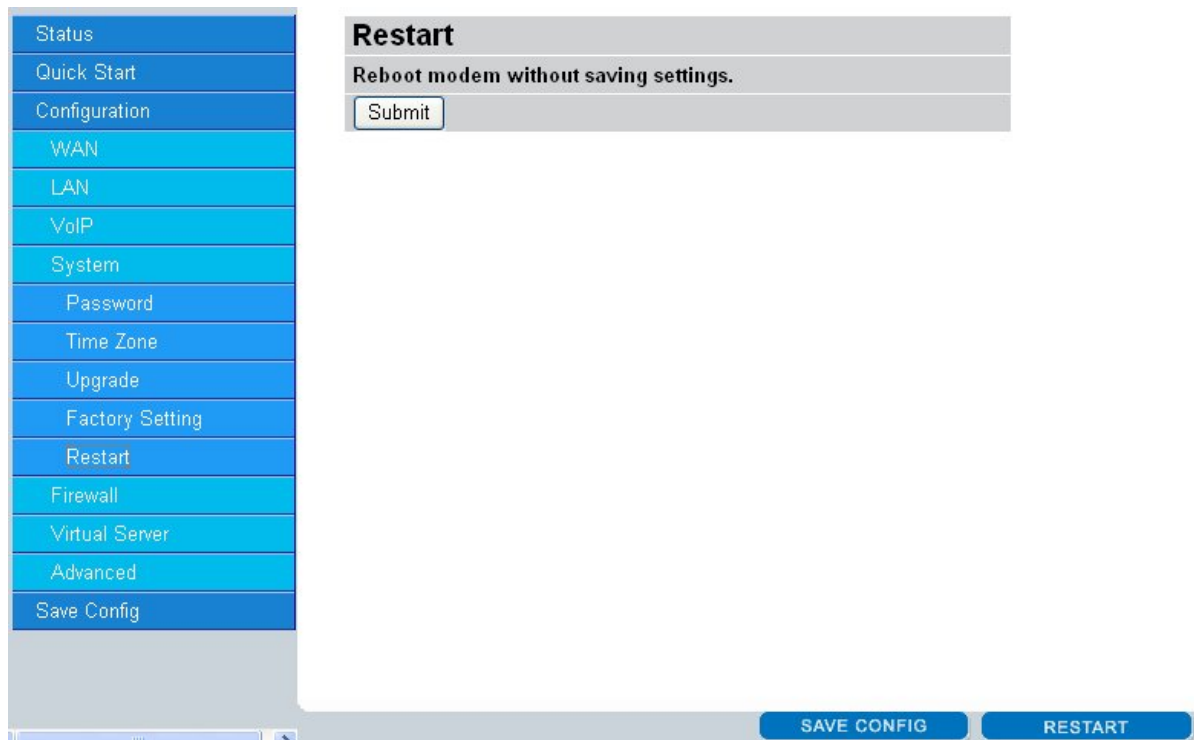
3.4.3.4.4 Factory Setting

If for any reason, you have to reset this router back to factory default settings, be careful that the current settings will be lost and the settings are reset back to its default value. The factory default values is detailed in the **section 3.2 “Factory Default Settings”**.



3.4.3.4.5 Restart

In case the router stops responding correctly or in some other way stops functioning, you can perform the restart. Your setting won't be changed. Performing the restart, click on the **Submit** button.

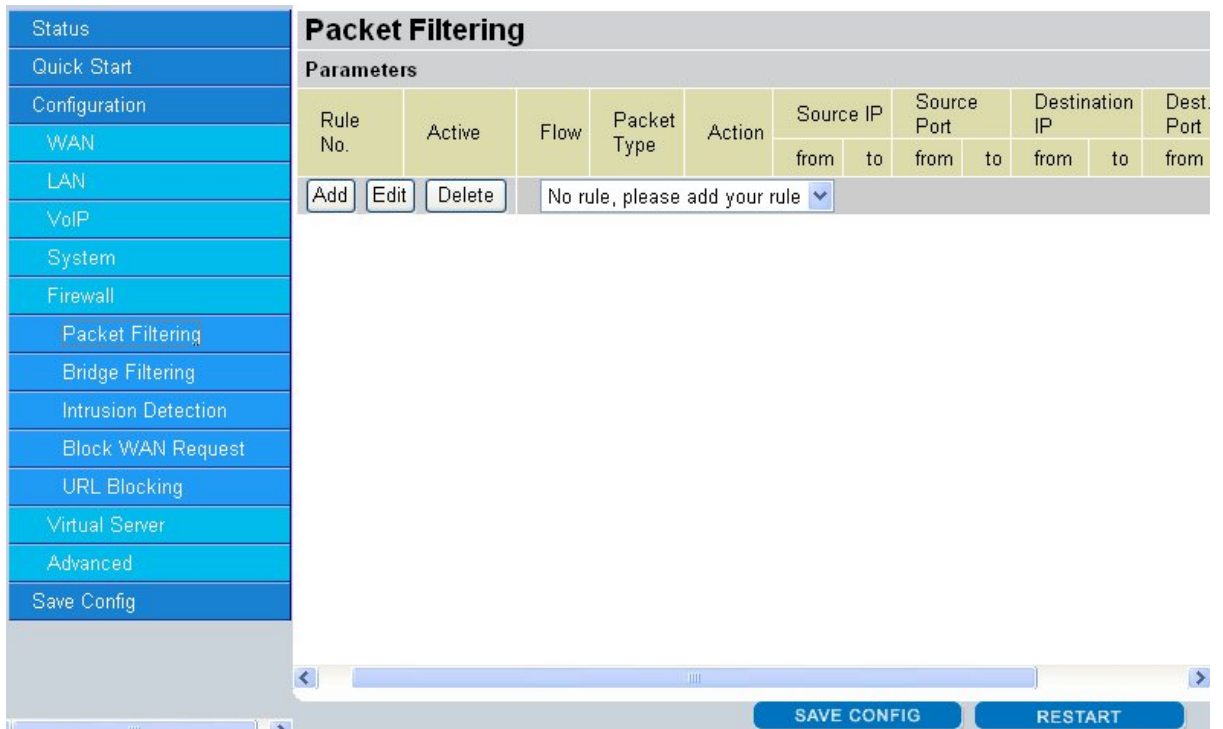


3.4.3.5 Firewall

User can decide to enable this firewall function including Packet Filter, Block Hacker Attack, and Block WAN request features for better security control or not. But be noted, it wastes network processor computation power. The performance will be lower about 10% to 15%. More firewall features will be added continually, please visit our web site to download latest firmware.

3.4.3.5.1 Packet Filtering

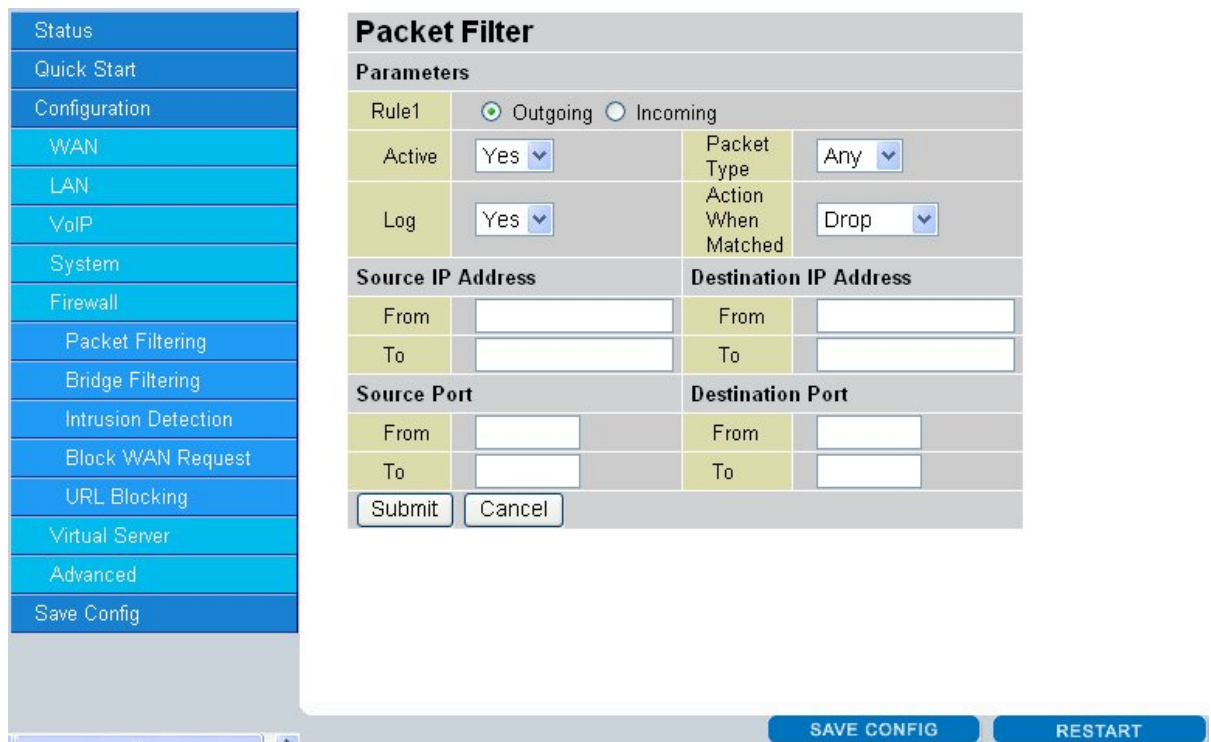
Packet filtering function enables you to configure your router to check specified internal/external user (**IP address**) from Internet access, or you can disable specific service request (**Port number**) to /from Internet. This configuration program allows you to set up different filter rules up to 6 for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation, which means the device checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Add: Click this button to add a new packet filter rule. After click, next figure will appear.

Edit: Check the Rule No. you want to edit. Then, click the “Edit” button.

Delete: Check the Rule No. you want to delete. Then, click the “Delete” button.



Outgoing **Incoming:** Determine whether the rule is for outgoing packets or for incoming packets.

Active: Choose “Yes” to enable the rule, or choose “No” to disable the rule.

Packet Type: Specify the packet type (TCP, UDP, ICMP or any) that the rule will be applied to.

Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

Log: Choose “Yes” if you want to generate logs when the filter rule is applied to a packet.

Action When Matched: If any packet matches this filter rule, **Forward** or **Drop** this packet.

Source IP Address: Enter the incoming or outgoing packet’s source IP address(es).

Source Port: Check the TCP or UDP packet’s source port number(s).

Destination IP Address: Enter the incoming or outgoing packet’s destination IP address(es).

Destination Port: Check the TCP or UDP packet’s destination port number(s).



If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of filtered private IP range in order to avoid conflicts because you do not know which PC in LAN is assigned to which IP address. The easiest and safest way is that the filtered IP address is assigned to specific PC that is not allowed to access outside resource such as Internet. You configure the filtered IP address manually to this PC, but it is still in the same subnet with the router.

3.4.3.5.2 Bridge Filtering

Bridge Filtering

Enable Bridge Filtering Yes No

ID	Src MAC*	Dest MAC*	Type**		
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Block	<input type="button" value="Add"/>
				<input type="radio"/> Forward	

* MAC address. Should look like 000002fa6fab.
 ** Ethernet type. Should look like a5ff.

SAVE CONFIG RESTART

Enable Bridge Filtering: Check **Yes** to enable this function or check **No** to disable.

Src MAC: Enter the source MAC address.

Dest MAC: Enter the destination MAC address.

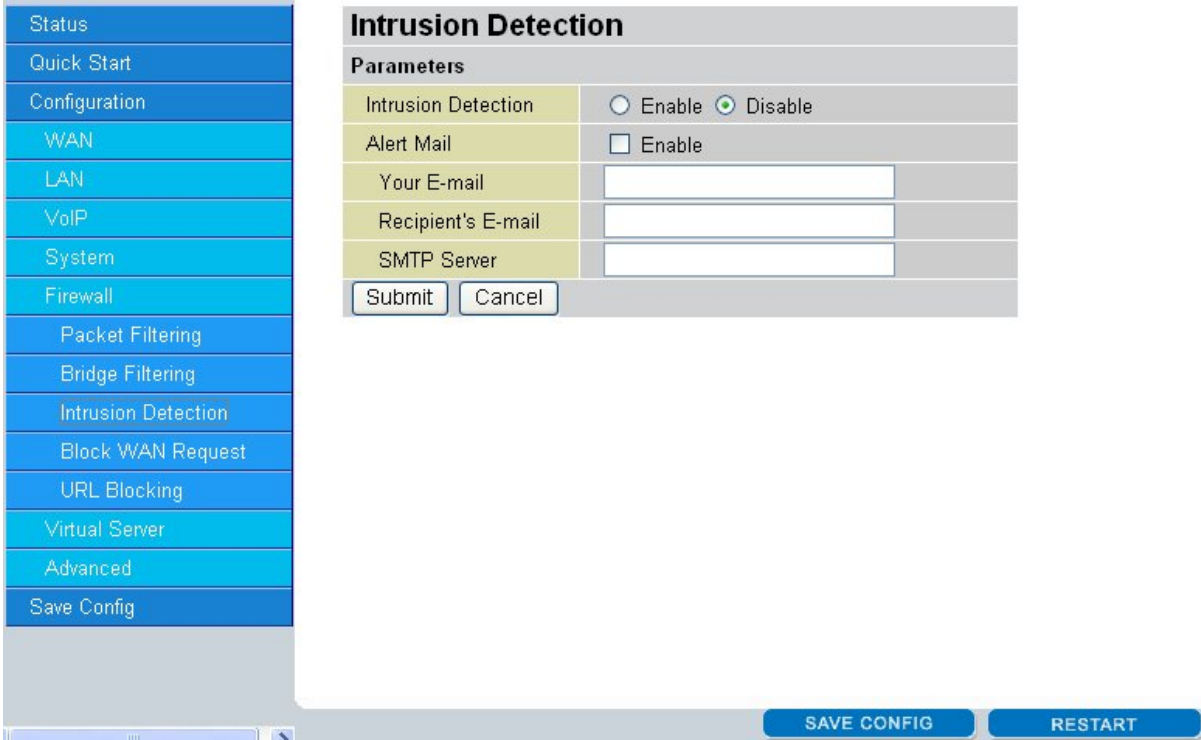
Type: Enter the Ethernet type.

Block **Forward:** Check **Block** if you want to block requests from the source MAC address sending to the destination MAC address. Check **Forward** if you want to forward requests from the source MAC address sending to the destination MAC address.

3.4.3.5.3 Intrusion Detection

Check "Enable" if you want to detect invader sneak in your computer without permitted .The ADSL Router can automatically detect and block the DoS (Denial of Service) attack if user enables this function. This kind of attack is not to achieve the confidential data of this network; instead, it aims to crush specific equipment or the entire network. If this happens, the users will not be able to access the network resources. There are few samples of hacker patterns implemented as below.

- **IP Spoofing**
- **Ping of Death (Length > 65535)**
- **Land Attack (Same source / destination IP address)**
- **IP with zero length**
- **Sync flooding**
- **Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)**
- **Snork Attack**
- **UDP port loop-back**
- **TCP NULL scan**



3.4.3.5.4 Block WAN Request

Check "Enable" if you want to exclude outside PING request from reaching on this router.



3.4.3.6 Virtual Server

The screenshot shows the 'Virtual Server Configuration' page. On the left is a navigation menu with items: Status, Quick Start, Configuration, WAN, LAN, System, Firewall, Virtual Server (highlighted), Advanced, and Save Config. The main content area is titled 'Virtual Server Configuration' and includes the instruction: 'Use the following form to add special port that you want to be opened for your special applica'. Below this is a table with columns: ID, Public Port (From), Public Port (To), Port Type, Map To, Host IP Address, and Private Port. The first row contains the value '1' in the ID column, empty fields for the other columns, and radio buttons for 'TCP' (selected) and 'UDP'. Below the table is an 'Information' section with the same column headers. At the bottom right, there are two buttons: 'SAVE CONFIG' and 'RESTART'.

ID	Public Port (From)	Public Port (To)	Port Type	Map To	Host IP Address	Private Port
1			<input checked="" type="radio"/> TCP <input type="radio"/> UDP	--->		

ID	Public Port (From)	Public Port (To)	Port Type	Map To	Host IP Address	Private Port
----	--------------------	------------------	-----------	--------	-----------------	--------------

Being a natural Internet firewall, the ADSL Router protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this product can act as a virtual server. You can set up a local server with specific port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), DNS (53), ECHO (7), NNTP (119). When an incoming access request to the router for specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Public Port number 21 (FTP) to be mapped to the IP Address 192.168.1.100, then all the ftp requests from outside users will be forwarded to the local server with IP address of 192.168.1.100.

ID	Public Port (From)	Public Port (To)	Port Type	Map To	Host IP Address	Private Port
4			<input checked="" type="radio"/> TCP <input type="radio"/> UDP	--->		

Information

ID	Public Port (From)	Public Port (To)	Port Type	Map To	Host IP Address	Private Port
1	21	21	TCP	--->	192.168.1.50	
2	80	80	TCP	--->	192.168.1.100	
3	23	23	UDP	--->	192.168.1.150	

SAVE CONFIG RESTART

Public Port (from) & Port (To): Enter the public port number & range you want to configure.

Port Type: Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

Host IP Address: Enter the IP address of certain internal server to which requests from the specified port is forwarded.

3.4.3.7 Advanced

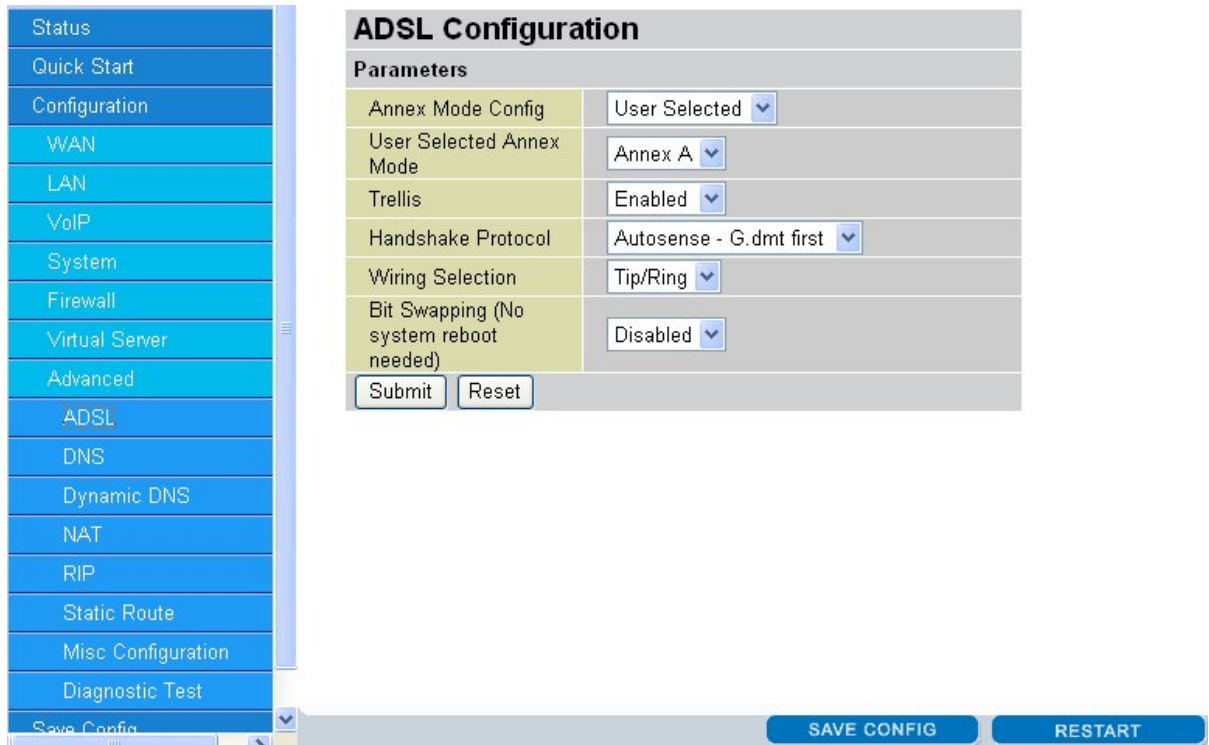
There are eight items under the **Advanced** section: ADSL, DNS, Dynamic DNS, NAT, RIP, Static Routing, MISC Configuration and Diagnostic Test.

3.4.3.7.1 ADSL

Trellis: Default at Enabled.

Handshake Protocol: Default at Autosense – G.dmt first. You can also choose other protocols, such as Autosense – T1.413 first, G.dmt/G.lite, T1.413, G.dmt, G.lite.

Wiring Selection: Default at Tip/Ring. Select Auto or A/A1 if necessary.



3.4.3.7.2 DNS

A Domain Name System (DNS) contains a mapping table for domain name and IP address. In the Internet, every host has a unique and friendly name such as www.yahoo.com and IP address. The IP address is so hard to remember that you may just enter the friendly name www.yahoo.com and then the DNS will convert it to its equivalent IP address.

You can obtain Domain Name System (DNS) IP address automatically if ISP provides it when you logon. Or your ISP may provide you with an IP address of DNS. If this is the case, you must enter the DNS IP address.

Status	<h3>DNS Configuration</h3> <p>Parameters</p> <p>DNS Proxy Selection <input type="checkbox"/> Enabled <input checked="" type="checkbox"/></p> <p>Auto Discovery <input checked="" type="checkbox"/></p> <p>User Configuration <input type="checkbox"/></p> <p>DNS Server <input type="text"/> Add <input type="button" value="Add"/></p> <p><input type="button" value="Submit"/> <input type="button" value="Cancel"/></p> <p>DNS Advanced configuration</p> <p>Information</p> <table border="1"> <thead> <tr> <th>#</th> <th>DNS Server's IP</th> </tr> </thead> <tbody> <tr> <td colspan="2">Number of User Defined DNS Proxy 0</td> </tr> </tbody> </table>	#	DNS Server's IP	Number of User Defined DNS Proxy 0	
#		DNS Server's IP			
Number of User Defined DNS Proxy 0					
Quick Start					
Configuration					
WAN					
LAN					
VoIP					
System					
Firewall					
Virtual Server					
Advanced					
ADSL					
DNS					
Dynamic DNS					
NAT					
RIP					
Static Route					
Misc Configuration					
Diagnostic Test					
Save Config					

3.4.3.7.3 Dynamic DNS

With Dynamic DNS service, a domain name can be translated into a dynamic IP address, which is often issued by ISP for dial-up service. A local server, such as Web server, Email server or FTP server, can then be easily accessed without knowing the changing IP address.

Status	<h3>Dynamic DNS</h3> <p>Parameters</p> <p>Dynamic DNS <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p><input type="text" value="www.dyndns.org (dynamic)"/> <input type="button" value="Add"/></p> <p>Host <input type="text"/></p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p> <p>Period <input type="text" value="28"/> <input type="button" value="Add"/></p> <p><input type="button" value="Submit"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
WAN	
LAN	
VoIP	
System	
Firewall	
Virtual Server	
Advanced	
ADSL	
DNS	
Dynamic DNS	
NAT	
RIP	
Static Route	
Misc Configuration	
Diagnostic Test	
Save Config	

Check the “Enable” button to access the Dynamic DNS service. You may sign up Dynamic DNS service at <http://www.dyndns.org> and there you can also register domain names.

Host: Enter one domain name you have registered.

User Name: Enter the username used for sign-up.

Password: Enter the password used for sign-up.

Period: Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, BIPAC 7100SV will take the same action automatically whenever the assigned IP changes

3.4.3.7.4 NAT

The **NAT Configuration** page allows the user to set the configuration for the Network Address Translation.

Session Name	User's IP	Action
<input type="text"/>	<input type="text"/>	Add <input type="button" value="v"/>

#	Session Name	User's IP
---	--------------	-----------

#	Session Name	Interface
---	--------------	-----------

Dynamic NAPT: It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based-on the destination IP addresses and Rout Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

NAT (Static): This option maps single WAN IP address to the local PC IP address. It is peer-to-peer mapping, one-to-one. For each WAN interface, only one local PC IP address can be associated with each WAN interface. Click the link **Session Name Configuration** to add the session name for WAN interface.

NAPT (Static): This option maps the single WAN IP address to many local PCs IP addresses, one-to-many. It is the multiple-mapping mechanism. For each WAN interface, more than one local PC can be

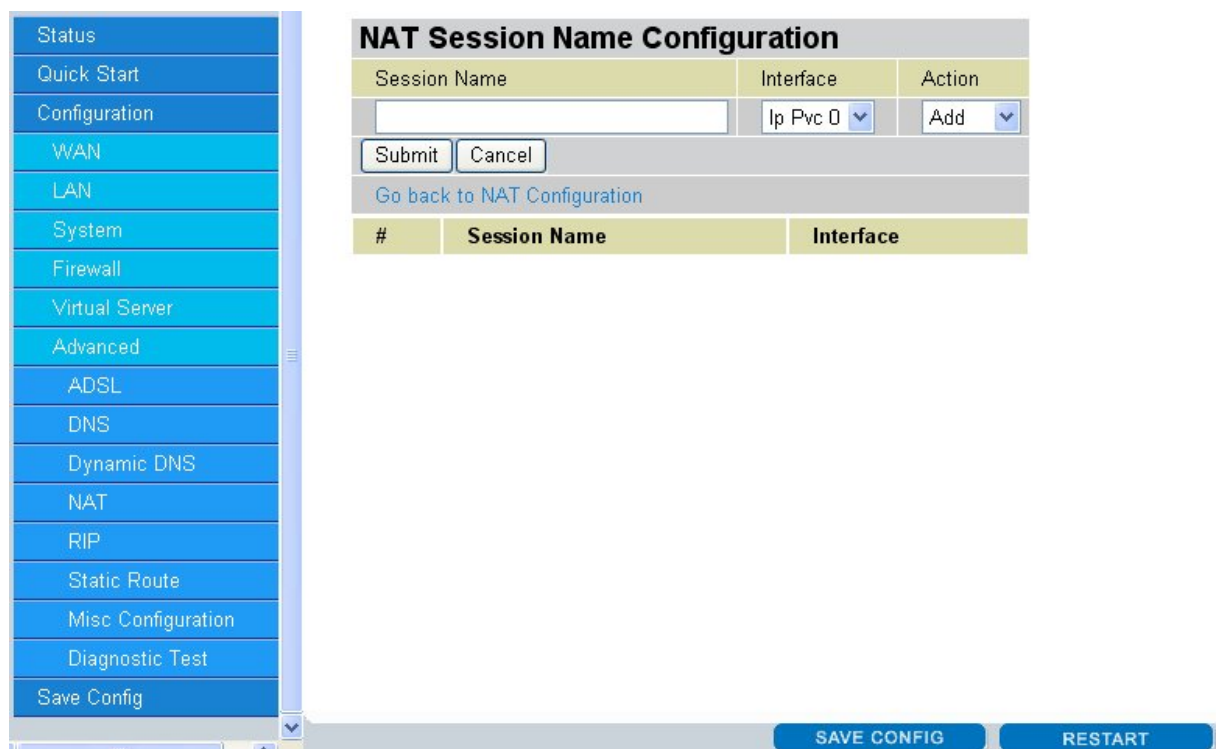
associated with one WAN interface. Click the **Session Name Configuration** to add the session name for WAN interface.

Session Name: Enter the desired session name.

User's IP: Allows the user to assign the IP address to map the corresponding NAT/NAPT sessions.

Session Name status will be displayed at the middle of this page to show the corresponding Session Name with its IP address.

Click **Session Name Configuration**, the following screen displays.



Session Name: Enter the desired session name.

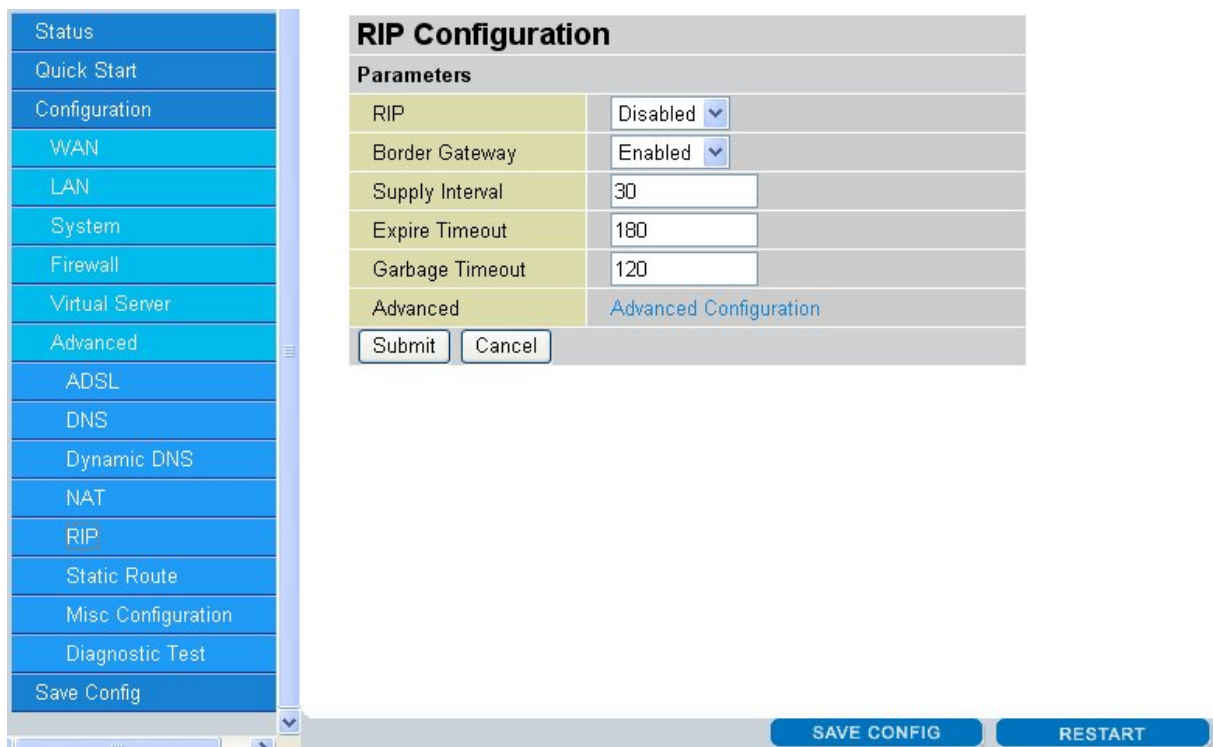
Interface: This field allows the user to choose specific WAN interface (PVC or PPP Session) for NAT session.

NAT allows only one entry (User IP) per session, NAPT allows many entries (User IPs) per session.

Select **Add** or **Delete** and then press the **Submit** button to add or delete any NAT session name setting to/from the following table.

Go back to the previous page, NAT Configuration, to continue further settings.

3.4.3.7.5 RIP



RIP: Default is **Disabled**.

Border Gateway: Default is **Enabled**.

Supply Interval **seconds:** The default value is 30 seconds.

Expire Timeout **seconds:** The default value is 180 seconds.

Garbage Timeout **seconds:** The default value is 120 seconds.

RIP Advanced Configuration

RIP Per Interface Configuration

Interface	Enabled?	Supplier	Listener
Ip Ethernet 0	No	Disabled	V1

Back to RIP Configuration

Submit Cancel

Current RIP Settings

#	Interface	Enabled?	Supplier Mode	Listener Mode
1	Ip Ethernet 0	No	V2 BC	V1+V2
2	Ip Usb 0	No	V2 BC	V1+V2
3	Ip Pvc 0	No	Disabled	V1+V2
4	Ip Pvc 1	No	Disabled	V1+V2
5	Ip Pvc 2	No	Disabled	V1+V2
6	Ip Pvc 3	No	Disabled	V1+V2
7	Ip Pvc 4	No	Disabled	V1+V2
8	Ip Pvc 5	No	Disabled	V1+V2
9	Ip Pvc 6	No	Disabled	V1+V2
10	Ip Pvc 7	No	Disabled	V1+V2
	Ip BridgeMux			

SAVE CONFIG RESTART

3.4.3.7.6 Static Route

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.

System Default Gateway Configuration

Parameters

Address Pool Selection

None
 Auto
 Select Interface Ip Ethernet 0
 Specify IP

Submit

Static Route Configuration

Destination	Netmask	Gateway
		<input checked="" type="radio"/> Specify IP <input type="radio"/> Select Interface Ip Ethernet 0

Add Submit Reset

Manually Configured Routes

#	Destination	Netmask	Gateway
---	-------------	---------	---------

SAVE CONFIG RESTART

Add: Click this button to add a new static routing. When you click this button, the next figure appears.

Delete: Check the item you want to delete. Then, click the “Delete” button.

Destination / Subnet Mask / Gateway Address: Fill in these fields required by this Static Routing function.

3.4.3.7.7 MISC Configuration

Miscellaneous Configuration	
Parameters	
HTTP Server Access	<input type="radio"/> All <input checked="" type="radio"/> Restricted
<input checked="" type="checkbox"/> LAN	
<input checked="" type="checkbox"/> WAN Specify IP	10.0.0.3
Subnet Mask	255.0.0.0
HTTP Server Port	80
HTTP Password Protection	Enabled
FTP Server	Enabled
	<input checked="" type="checkbox"/> Disable WAN side FTP access
TFTP Server	Disabled
DMZ	Disabled
DMZ Host IP	0.0.0.0
DHCP Relay	<input type="radio"/> NONE <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay
DHCP Relay Target IP	0.0.0.0
IGMP Proxy	Disabled
PPP Half Bridge	Disabled
PPP Reconnect on	Disabled

HTTP server access: Default at **Restricted**.

HTTP server port: Default at **80**.

FTP server: Default at **Enabled**.

TFTP server: Default at **Disabled**.

DMZ: Regarding the DMZ Host, it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by NAT algorithms in the ADSL Router, then passed to the DMZ host when the packet is not sent by hacker or not limited by the virtual server list.

DMZ HOST IP: Enter the IP address of the DMZ host.

DHCP Relay: Default at **DHCP Server**.

DHCP Target IP: Default is **0.0.0.0**

IGMP Proxy: Default at **Disabled**.

PPP Half Bridge: Default at **Disabled**.

PPP reconnect on WAN access: Default at **Disabled**. Select **Enabled** if you want to automatically re-establish the PPPoE/PPPoA session when disconnected by ISP.

3.4.3.7.8 Diagnostic Test

As soon as you enter the test program, all tests will run automatically to diagnose the connection status of the device.

Results		
Diagnostic Test		
Checking LAN Connection		
Testing Ethernet LAN connection	PASS	HELP
Checking ADSL Connection		
Testing ADSL Synchronization	FAIL	HELP
Checking Circuit 0 for Network Connection		
Test ATM OAM Segment Loop Back	SKIPPED	HELP
Test ATM OAM End-to-End Loop Back	SKIPPED	HELP
Test Ethernet connect to ATM	SKIPPED	HELP
Test IP connect to Ethernet	SKIPPED	HELP
Testing Internet Connection		
Ping primary DNS	SKIPPED	HELP
Query DNS for www.google.com	SKIPPED	HELP
Ping www.google.com	SKIPPED	HELP

Checking LAN Connection

Testing Ethernet LAN connection

This test passes if the Ethernet LAN interface is working properly.

Checking ADSL Connection

Testing ADSL Synchronization

This test checks your DSL modem to see if it can successfully negotiate and establish a DSL connection with your service provider's central office equipments. The test returns PASS if a DSL connection is established.

If this test returns FAIL, please try the test again a few minutes after this test is completed. Since your DSL modem need a couple of seconds to a few minutes to establish the DSL connection depending on your phone line quality. If this test returns FAIL, make sure your phone line is connected to your DSL modem securely, and also check with your service provider to see if your service is activated.

If this test returns FAIL, all other tests will be skipped.

Checking Circuit 0 for Network Connection

Test ATM OAM Segment Loop Back

This test sends ATM OAM F5 Segment loop back request cells to the central office equipments through your DSL connection. This test will pass if response cell is received. Since your service provider might not support this test, your DSL modem could still work even if this test fails.

If this test fails consistently and your DSL modem seems not working, check to make sure the VPI and VCI are configured correctly.

This test returns FAIL if the DSL synchronization test failed.

Test ATM OAM End-to-End Loop Back

This test sends ATM OAM F5 End-to-End loop back request cells to the central office equipments through your DSL connection. This test returns PASS if response cell is received. Since your service provider might not support this test, your DSL modem could still work even if this test fails.

If this test return FAIL consistently and your DSL modem seems not working, check to make sure the VPI and VCI are configured correctly.

This test returns SKIPPED if the DSL synchronization test failed.

Test Ethernet connect to ATM

This test returns PASS if the ATM AAL5 module is loaded correctly in your DSL modem. If this test returns FAIL, an internal error has occurred.

This test returns SKIPPED if the DSL synchronization does not return PASS.

Test IP connect to PPP

This test returns PASS if your DSL modem has been assigned a valid IP address by your service provider through DHCP or your DSL modem is assigned a valid IP address statically.

If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and DHCP client is turned on in your DSL modem, check with your service provider. If this test returns FAIL consistently and your DSL modem is statically assigned an IP address, make sure the IP address is the correct one assigned by your service provider.

This test returns SKIPPED if "Ethernet connect to AAL5" test does not return PASS.

Test Internet connection

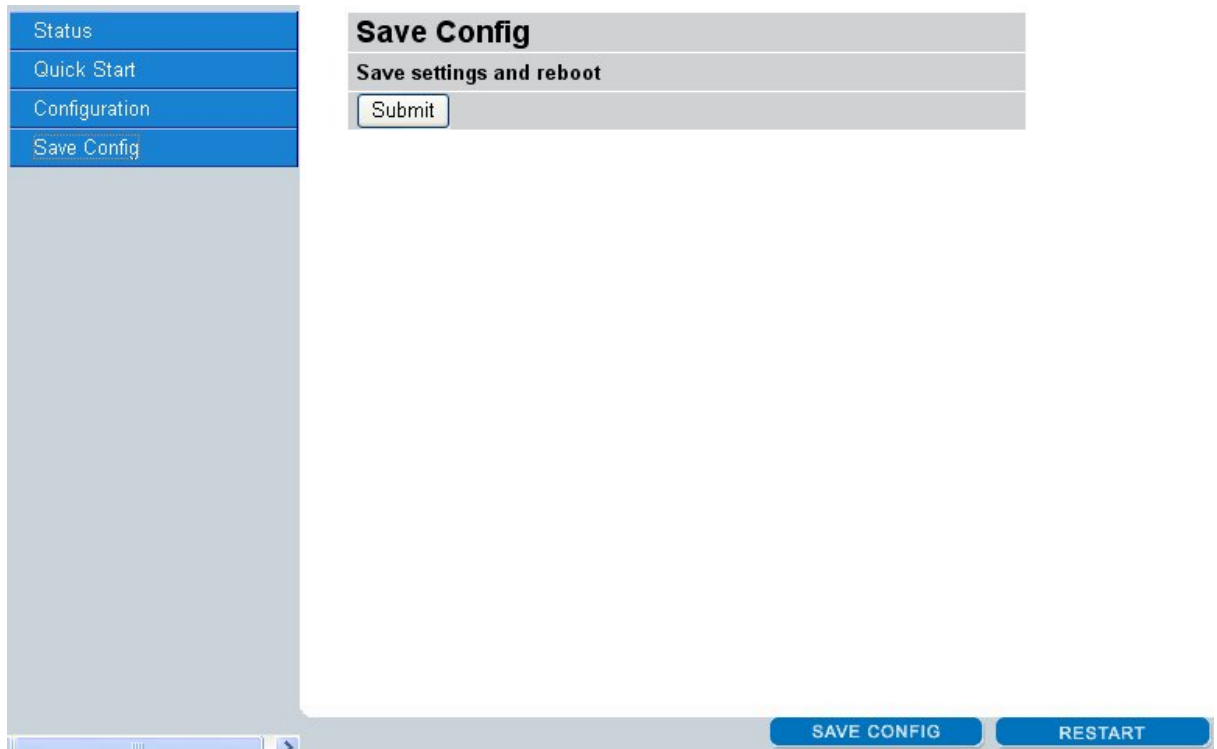
This test returns PASS if the gateway can be reached through ping request. The gateway is assigned by your service provider, or obtained from your service provider by PPP negotiation or DHCP negotiation.

If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your DSL modem seems not working, check to make sure your statically assigned IP address is configured correctly or DHCP client is turned on with the current VC.

This test returns SKIPPED if "IP connect to PPP" or "IP connect to Ethernet" test does not return PASS.

3.4.4 Save Config

Click the **Submit** button to write settings to flash. Then, the system will reboot for changes to take effect.



Chapter 4

Troubleshooting

If the ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems Starting Up the ADSL Router

Problem	Corrective Action
None of the LEDs are on when you turn on the ADSL Router.	Check the connection between the adapter and the ADSL Router. If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL SYN LED on the front panel of the ADSL Router should be on. Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP. Reboot the ADSL Router. If you still have problems, you may need to verify these variables with the telephone company and/or ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the LAN LNK LED on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your ADSL Router and the station.
	Verify that the IP address and the subnet mask are consistent between the ADSL Router and the workstations.

Problems Connecting to a Remote Node or ISP

Problem	Corrective Action
Can't connect to ISP.	Check section 3.4.1.3 "Status – PPP status" to verify the line status.

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

AUSTRALIA

<http://www.billion.com.au/>

Hotline: 1300 139 159, 7 days a week.

©2004 Billion Electric Co., Ltd. PC Range P/L. All Rights Reserved.

WORLDWIDE

<http://www.billion.com/>